Subscriber Data Management

Release 9.0

Product Description

910-6543-001 Revision B
December 2012

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter provides general information about manual organization, the scope of this manual, its targeted audience, how to get technical assistance, and how to locate customer documentation on the Customer Support site.

About this document

The Subscriber Data Management (SDM) *Product Description* document provides an overview and technical information about the Tekelec SDM product. The document describes the SDM system, its software, high availability and fault management, system configuration and subscriber provisioning, performance management, security management, a description of the hardware with FRU ordering information, and technical specifications.

Document organization

The information in this document is organized under these chapters:

- *Introduction* contains general information about this document, how to contact the Tekelec Customer Care Center, and how to locate the customer documentation on the Customer Support site.
- *System description* describes the Subscriber Data Management (SDM) architecture, its applications, interfaces used by the applications, and application features. In addition, this chapter describes high availability (HA) and fault management, system configuration and subscriber provisioning, security management, as well as performance management and the hardware platforms.
- *Software description* describes the software architecture, system and subscriber management, and application features.
- *High availability* describes how the SDM system provides high availability.
- *Fault management* describes fault management of the SDM OAM&P subsystem, including SNMP and database backup and restore.
- *Configuration management* describes the configuration management software, which provides features to
  - list the identity, the type, and parameters of a configuration
  - define default values
  - modify operating characteristics

  System provisioning and configuration management is provided via the CLI and WebCI interfaces.
- *Subscriber provisioning* describes subscriber provisioning via the CLI and WebCI interfaces. New subscriber profiles can be added. Existing subscribers can be modified, deleted, or displayed. Services associated with each subscriber can also be added, modified, deleted, or displayed
- *Performance management* describes counters, which allow the operator to manage system performance.
- *Security management* describes the various levels of security to prevent unauthorized access to the system.
- *Hardware description* describes the supported hardware platform and its hardware components.
- *Technical specifications* provides technical specifications for the Subscriber Data Management system.

About links and references

Information within the same document is linked and can be reached by clicking the hyperlink.

To follow references pointing outside of the document, use these guidelines:

General:

- Locate the referenced section in the Table of Content of the referenced document.
- Locate the same section name in the referenced document.
- Place the PDF files in one folder or on a disc and use the powerful Adobe PDF search functions to locate related information in one or more documents simultaneously.

Alarms

- *SDM Alarms Dictionary*

Product, features, concepts

- *SDM Product Description*

Monitoring, maintenance, or troubleshooting:

- Procedures: *Monitoring, Maintenance, Troubleshooting User Guide*
- Entities: *Monitoring, Maintenance, Troubleshooting Reference Manual*

Subscriber provisioning:

- Procedures: *Subscriber Provisioning User Guide*
- Entities: *Subscriber Provisioning Reference Manual*

System configuration:

- Procedures: *System Configuration User Guide*
- Entities: *System Configuration Reference Manual*

User Interfaces:

- *User guides*
  - How to use the user interface
  - How to set up users (permissions, groups, services)
- *Reference manuals*
  - About user interfaces
  - Entities for setting up users

To determine the components of the complete documentation set delivered with the software, refer to the *SDM Documentation Roadmap* delivered with each documentation set.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)

	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Related publications

For a detailed description of the available SDM documentation, refer to the *SDM Documentation Roadmap* included with your SDM documentation set.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

  Phone:

  0-800-555-5246 (toll-free)
- **Brazil**

  Phone:

  0-800-891-4341 (toll-free)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays
- **Chile**

  Phone:

  1230-020-555-5468
- **Colombia**

  Phone:

  01-800-912-0537
- **Dominican Republic**

  Phone:

  1-888-367-8552
- **Mexico**

  Phone:

  001-888-367-8552
- **Peru**

  Phone:

  0800-53-087
- **Puerto Rico**

  Phone:

  1-888-367-8552 (1-888-FOR-TKLC)
- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Signaling**

  Phone:

  +44 1784 467 804 (within UK)

- **Software Solutions**

  Phone:

  +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

    +91 124 436 8552 or +91 124 436 8553

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with the Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

System description

Topics:

This chapter describes the Subscriber Data Management (SDM) architecture, its applications, interfaces used by the applications, and application features. In addition, this chapter describes high availability (HA) and fault management, system configuration and subscriber provisioning, security management, as well as performance management and the hardware platforms.

Introduction

The Tekelec Subscriber Data Management (SDM) product family is a multi-profile subscriber management system, designed with an objective to consolidate all the information (or profiles) of a mobile subscriber. It enables centralization of subscriber information/data in one logical place and convergence of subscriber's registration, authentication and call termination at the core of the network, regardless of the access domain (including GSM/UMTS, IMS, SIP, LTE, and others).

The SDM product family combines both the Tekelec Nextgen Home Location Register (ngHLR) and the Home Subscriber Service (HSS) products. Built on SDM, the ngHLR product includes an integrated Authentication Centre (AuC) and Session Initiation Protocol (SIP) Registrar and Domain Selection Function (DSF) as well as a SIP Redirect server and a GSM Registration Agent, all running on a scalable, dynamic and secure system and within a single subscriber management platform. Such implementation enables a range of innovative solutions such as advanced low-cost roaming and HLR-based Fixed Mobile Convergence (FMC).

The Tekelec Home Subscriber Server HSS provides access to IMS services from multiple network types. The Tekelec ngHLR/HSS combination enables the creation and management of a single subscription with an unlimited number of profiles. Moreover, the SDM can run in a Geo-Redundant deployment. The SDM product family also supports the functionalities of an Authentication, Authorization and Accounting (AAA) Server, as well as equipment identity checks through the Equipment Identity Register (EIR).

Network applications

The evolved Subscriber Data Management (SDM) solution features a distributed and layered architecture that provides a scalable back-end database, the Subscriber Data Server (SDS), which centralizes subscriber data from multiple front ends such as these applications: 3GPP ngHLR and AuC functions, MNP, SIP-AS, IMS-HSS, LTE-HSS, EIR, LTE-EIR, ENUM, 3GPP AAA (WiMAX AAA), and SPR. In other releases, it can also include other functional elements, or network applications, as depicted in this figure.

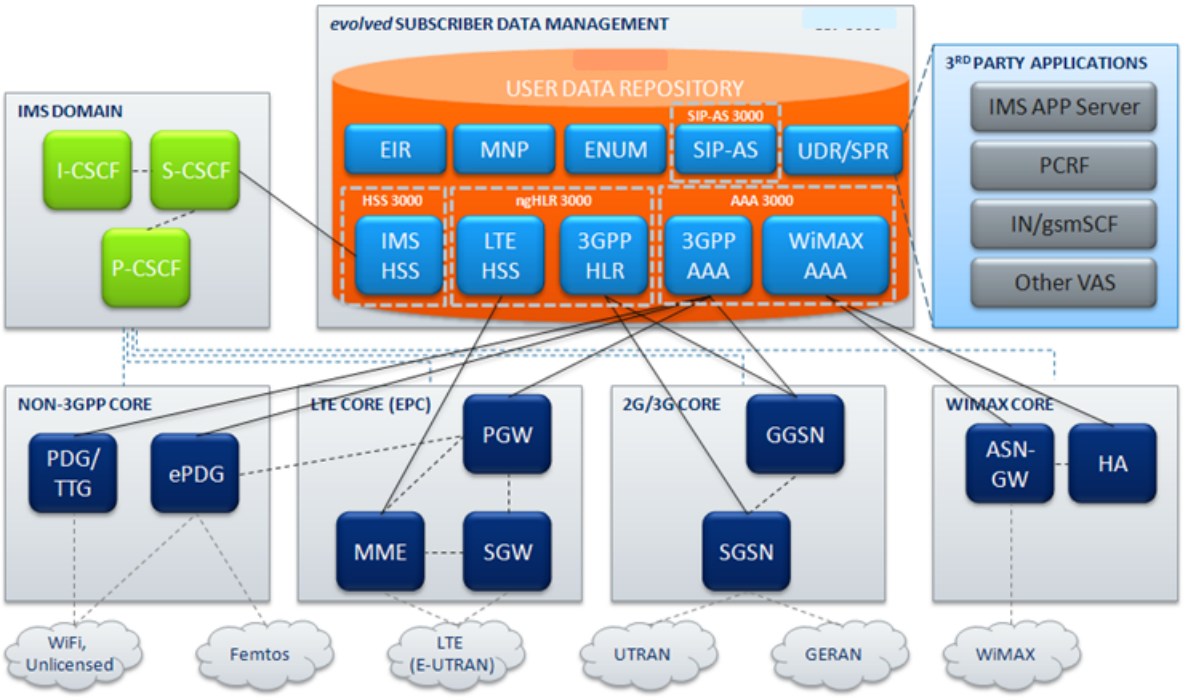


Figure 1: The SDM and typical network architecture

Tekelec Next Generation Home Location Register (ngHLR)

The Home Location Register (HLR), as defined by the Third Generation Partnership Project (3GPP) serves as the primary database repository of subscriber information within GSM/GPRS networks. Combined with an integrated Authentication Center (AuC), it provides a central point for registration and authentication of mobile subscribers, while also acting as the real-time location repository for routing of incoming calls and Short Messages (SMS). The HLR/AuC supports the MAP (Mobile Application Part) protocol over an SS7 interface. Thanks to its multi-profile subscriber database and dynamic association engine, the Tekelec ngHLR is capable of supporting multiple GSM identities and mobile phone numbers for any given subscription; such patent-pending capability is at the foundation of HLR-based advanced low-cost roaming solutions. Based on the SDM, the HLR benefits from linear scaling through a next-generation architecture by simply adding additional Single Board Computer (SBC) to the system.

LTE-HSS

The Long Term Evolution-Home Subscriber Server (LTE-HSS), as defined by the 3rd Generation Partnership Project's (3GPP) LTE wireless communication standard, serves as the primary database repository of subscriber information within Evolved Packet Core (EPC) (also known as the System Architecture Evolution (SAE)) networks. The LTE-HSS exchanges messages with an MME or a SGSN using the Diameter Protocol (defined by the IETF in the RFC3588) over TCP or SCTP. The LTE-HSS serves as a registration and authentication of mobile subscribers in the EPC network, while also tracking their mobility by acting as the real-time location repository and updating their position in administrative areas handled by MMEs/SGSNs. The LTE-HSS is also responsible for sending the subscriber data profile to a MME/SGSN when a subscriber first roams there and for removing the subscriber data from the previous MME/SGSN when a subscriber has roamed away from it. The SDM system's

LTE-HSS is 3GPP Release 9 compliant and has been fully integrated with the GSM/UMTS ngHLR, which means that it shares the following with the Tekelec ngHLR:

- subscriber profile
- volatile data
- AuC
- SW/HW platform
- provisioning stream

The LTE-HSS is capable of supporting authentication and bidirectional roaming between 3G-LTE networks by either communicating with the SDM ngHLR or with the SDM ngHLR's HLR-proxy functionality to forward messages to a legacy HLR.

SIP-AS

SIP Registrar

The SIP Registrar functional element is integrated within the Tekelec ngHLR. Compatible with IETF (Internet Engineering Task Force) standards, the SIP Registrar plays a similar role in SIP based, Voice-over-IP (VoIP) networks as the 3GPP HLR/AuC plays in GSM networks. Subscribers with a VoIP subscription, either via a SIP phone, terminal adapter, dual-mode handset or simple SIP software client, can access voice services by registering and authenticating with a Registrar. Soft-switches and Proxies can then query the Registrar to obtain the Contact URI (Uniform Resource Identifier) associated with the public Address-of-Record (AoR).

Domain Selection Function

The Domain Selection Function element is also integrated within the Tekelec ngHLR. Its role is to provide an intelligent, routing decision point for incoming voice calls destined to a multi-mode subscriber, thus seamlessly solving one inherent problem of Fixed Mobile Convergence: the Network Domain Selection. When the HLR receives a MAP message requesting for a subscriber's location, the DSF determines the optimal routing destination based on the registration status of the subscriber (GSM-only, SIP-only, GSM and SIP), the subscriber preferences, and the operator's preferences. The DSF provides the same services for calls coming from the VoIP domain into the SIP Redirect Server. In future releases, the DSF will evolve to comply with the 3GPP IMS Voice Call Continuity (VCC) framework.

SIP Redirect Server

The SIP Redirect Server functional element is integrated within the Tekelec ngHLR and provides a traditional SIP Redirect Server functionality (as described in RFC 3261) augmented with domain selection. The SIP redirect server with SIP-anchored domain selection provides the ability to process a SIP Invite request and return a SIP Redirect response which provides contact information for the subscriber. Subscribers may be SIP-only subscribers, GSM-only or dual-mode subscribers (SIP and GSM). The SIP Redirect server performs authorization of Invite requests but does not perform authentication. GSM, SIP and other temporary contact types allow the Tekelec ngHLR to perform call mediation when responding to SIP Invite requests.

GSM Registration Agent

In the SIP-anchored FMC + GSM registration agent model, the primary network registrar is located in the SIP domain (this can be either an IMS network or a pre-IMS SIP network). In this case, the

Tekelec ngHLR acts as a gateway between the GSM mobile network and the SIP network. The responsibility of the Tekelec ngHLR is to provide the IMS network or the pre-IMS SIP network with contact information for GSM mobile subscribers.

This is achieved by performing a SIP Register/Deregister for each GSM subscriber, thereby making non-SIP GSM devices appear to be valid SIP endpoints, with SIP contact information. The GSM registration agent is the element used to register GSM subscribers with an external SIP registrar. The GSM registration agent relies on the SIP Redirect Server integrated in the Tekelec ngHLR to process incoming Invite requests. To achieve this, the registration contact info provided is the SIP Redirect Server contact Info.

IMS Home Subscriber Server (IMS-HSS)

Serving as the Home Subscriber Server (HSS) function in 3GPP IP Multimedia Subsystem (IMS), the HSS is the central subscriber database for next generation IP and GSM networks. In line with the evolution of the HLR in the IMS standardization and facilitating a controlled migration to 3GPP-defined networks, the Tekelec ngHLR/HSS combination enables the creation and management of one converged profile per subscriber. The HSS design follows a distributed database model servicing both IMS Applications (CSCF) and GSM Applications (HLR

Subscription Locator Function (SLF)

The SLF functional element is integrated within the HSS and provides a traditional Subscription Locator Function functionality. The SLF functionality is needed in a multi-HSS deployment and can be configured and provisioned in the HSS as it is implemented within the HSS process. Its role is to redirect Diameter queries from the CSCF or SIP Application Servers to the right Home Subscriber Server.

ENUM Server

The ENUM Server is a DNS server integrated within the HSS. The ENUM Server (Electronic Number Mapping from E.164 Number Mapping) provides the support for the telephone number mapping functionality. It uses special DNS record types to translate a telephone number into a Uniform Resource Identifier (URI) or IP address that can be used in Internet communications.

Authentication, Authorization and Accounting Server (AAA)

The AAA Server is a RADIUS server integrated within the HSS. It provides Authentication and Authorization services to RADIUS enabled network access servers (NAS), such as GGSNs, Dial-up servers, etc. The AAA also provides the IP address allocation function. Depending on configuration, the AAA server can provide dynamic or static IP address allocation to users. The IP addresses are selected from pre-configured Address allocation policies and based on selection criteria retrieved from the RADIUS message. The AAA server is able to receive and respond to RADIUS Accounting messages and can be configured to proxy them to pre-configured Accounting servers. The AAA server does not store RADIUS accounting data.

Subscription Profile Repository (SPR)

The Tekelec Subscriber Data Server (SDS) runs the SPR functionality to act as a centralized system used for the storage of subscriber policy control data. The SPR can be deployed in environments where PCRF nodes need access to a separate repository for subscriber data. This data includes:

- Profile data: pre-provisioned information that describes the capabilities of each subscriber
- Quota data: information that represents the subscriber's use of managed resources
- State data: subscriber-specific properties

The SPR shares hardware, software, database, and provisioning stream (OAM&P) with all other applications running on the system (i.e., Tekelec ngHLR, SIP-AS, LTE-HSS). The PCRFs communicate with the SDM IMS-HSS front-end application over the Sh interface to write/query/update the subscriber policy data. The SPR handles the policy profile as an IMS-HSS profile.

For more details on the SPR functionality and its features, refer to “SPR Functionality”.

Interfaces

Tekelec ngHLR interfaces

The Tekelec ngHLR supports SS7 interfaces.

SS7 interfaces

A number of SS7/MAP-based interfaces and reference points connect the HLR/AuC with various entities in the GSM Circuit-Switched and GPRS Packet-Switched domains as shown in *Figure 2: SPR Sh connectivity*. These interfaces are defined in Technical Specification TS 29.002 [1]. These interfaces and reference points allow for control between the Tekelec ngHLR and the following entities in the network:

- *C Interface* - The Gateway MSC server interrogates the HLR of the required subscriber to obtain routing information for a call or a short message directed to that subscriber. Signaling on this interface uses the Mobile Application Part (MAP), which in turn uses the services of Transaction Capabilities (TCAP). The interface is used at terminating calls to exchange routing information, subscriber status, location information, and subscription information.
- *D Interface* -This interface is used to exchange the data related to the location of the mobile station and to the management of the subscriber. The main service provided to the mobile subscriber is the capability to set up or to receive calls within the whole service area. To support this, the location registers have to exchange data. Exchanges of data may occur when the mobile subscriber requires a particular service, when they want to change some data attached to his subscription or when some parameters of the subscription are modified by administrative means. Signaling on this interface uses the Mobile Application Part (MAP), which in turn uses the services of Transaction Capabilities. For CAMEL purposes, this interface is used to send the CAMEL related subscriber data to the visited PLMN and to provision the MSRN (Mobile Station Roaming Number).
- *Gc Interface* - This signaling path may be used by the GGSN to retrieve information about the location and supported services for the mobile subscriber, to be able to activate a packet data network address.

  There are two alternative ways to implement this signaling path:

  - if an SS7 interface is implemented in the GGSN, signalling between the GGSN and the HLR uses the Mobile Application Part (MAP), which in turn uses the services of Transaction Capabilities (TCAP).

  - if there is no SS7 interface in the GGSN, any GSN in the same PLMN and which has an SS7 interface installed can be used as a GTP to MAP protocol converter, thus forming a signalling path between the GGSN and the HLR.

- *Gr Interface* - This interface is used to exchange the data related to the location of the mobile station and to the management of the subscriber. The main service provided to the mobile subscriber is the capability to transfer packet data within the whole service area. The SGSN informs the HLR of the location of a mobile station managed by the latter. The HLR sends to the SGSN all the data needed to support the service to the mobile subscriber. Exchanges of data may occur when the mobile subscriber requires a particular service, when they want to change some data attached to their subscription or when some parameters of the subscription are modified by administrative means. Signaling on this interface uses the Mobile Application Part (MAP), which in turn uses the services of Transaction Capabilities (TCAP).
- *CAMEL gsmSCF Interface* - This interface is used by the gsmSCF to request information from the HLR. As a network operator option the HLR may refuse to provide the information requested by the gsmSCF. This interface is also used for USSD operations, both for gsmSCF-initiated dialogues and MS-initiated dialogues (relayed via HLR). It is a network operator option whether to support or not USSD operations on this interface.

SIP-AS interfaces

A SIP-based interface and reference point connects the SIP Registrar, the SIP Redirect Server and GSM registration agent with an entity in the Pre-IMS SIP Domain or in the IMS domain. A SIP client, such as a SIP Proxy and a SIP UA in the pre-IMS SIP Domain, or a CSCF in an IMS Domain, interacts with the SIP Registrar, the SIP Redirect Server, and the GSM registration agent by sending SIP requests, also known as "methods", via the SIP interface. Signaling on this interface uses the Session Initiation Protocol (SIP) as defined in the IETF specification RFC 3261. The SIP interface of the Tekelec ngHLR is used for registration and deregistration as well as for retrieving information on registrar capabilities. Therefore, five SIP requests can be sent via this interface:

- *SIP Register* - A SIP UA sends this "method' to the SIP Registrar to register and deregister its location, which the SIP Registrar stores in its database and acts as the location service.
- *SIP Options* - A SIP UA sends this "method" to the SIP Registrar to determine either the registrar's capabilities or its availability for service.
- *SIP Invite* - A SIP UA sends this "method" to the SIP Redirect Server to request a SIP Invite session.
- *SIP Cancel* - A SIP UA sends this "method" to the SIP FMC Server to cancel a pending request.
- *SIP ACK* - A SIP UA sends this "method" to the SIP Redirect Server to confirm that the client has received a final response to an Invite request.

The FMC feature uses a single IP address, which is shared by the Sip Server (Registrar and Redirect Server) and the GSM Registration agent (SipUa), but they use different ports.

HSS interfaces

This section provides an overview of the Diameter network interfaces supported by the HSS.

IP Interfaces

The HSS supports the ENUM Server, which communicates with a PABX or Gateway through an interface using the IP protocol. The messages supported are the following:

- DNS Queries containing a NAPTR NDS Record

- DNS Answers, as per the RFC3403

Through this interface, the PABX or Gateway can communicate with the SDM's ENUM Server in order to get the IP address of the destination by simply providing the telephone number (E.164) of the destination. This allows the Gateway to route a call from the SS7 network (PSTN) to an IP network (pre-IMS or IMS networks).

Diameter interfaces

The HSS currently supports the Cx/Dx and Sh/Dh interfaces, whereas in the next releases, all of the following interfaces will be supported as well: Si, Zh, Wx, Dw.

Diameter for Tekelec HSS provides a simple interface for Cx and Sh interface access to the HSS module. It also provides a simple interface for Dx and Dh interface access to the SLF functionality in the HSS module. To the HSS application module, it provides a simple interface from which to use the Cx/Dx and Sh/Dh interfaces.

To the network, it provides all of the necessary addressing and failover-recovery mechanisms required by the Cx/Dx and Sh/Dh interfaces. The HSS supports an IP based interface for communication with the Call Session Control Function (CSCF) and Application Server (AS) network elements as part of the IMS infrastructure. The Cx/Dx interfaces are specified on 3GPP Technical Specification TS 29.228 [13] and TS 29.229 documents[14]. The Sh/Dh interfaces are specified on 3GPP Technical Specification TS 29.328 [20] and TS 29.329 [21]. The four following distinct interfaces reference points are identified for the HSS on the IMS network:

ENUM server interface description

Among the several functionalities the HSS supports, the Enum Server functionality allows the HSS to achieve Telephone number mapping using the following interface:

- *PABX or Gateway/HSS (Enum Server) interface*

  This interface allows communication between the Tekelec HSS's Enum Server functionality and PABX or Gateways in order to allow to achieve DNS-based telephone number mapping, which consists of the translation of a telephone number into a Uniform Resource Identifier (URI) or IP address that can be used in Internet communications. For more details on the ENUM Server functionality, refer to *ENUM support*

The messages exchanged are the following:

DNS query:

```
The HSS supports DNS queries containing NAPTR DNS Records coming from a PABX or
Gateway in a SS7 network.
```

Note: The ENUM Server is only able to accept DNS Queries for Record NAPTR. All DNS messages other than DNS Queries set with a Question for Record NAPTR are not accepted, which means that the Enum Server sends back a DNS Answer with DNS NOT_IMPLEMENTED.

A DNS Query is sent in the form of a dotted Internet address, which is built from the telephone number and the domain name. For example, the fully qualified telephone number 1-315-567-1234 would turn into 4.3.2.1.7.6.5.5.1.3.1.e164.arpa. The digits are reversed because DNS reads right to left. The top level domain such as .com (or in this example: .arpa) in a URL is read first.

DNS answer:

```
The Enum Server builds the DNS Answer to send back to the quering PABX or Gateway.
```

AAA interface description

This section provides an overview of the RADIUS network interfaces supported by the AAA Server within the HSS.

RADIUS interfaces

The AAA Server supports a RADIUS interface over IPv4 UDP connections as specified in RFCs 2865, 2866 and 3576 and 3GPP TS 29.061. RADIUS interfaces.

In a GSM environment, the AAA Server interworks with a GGSN over the Gi interface, while in a non-3GPP traditional IP network, the AAA Server typically interworks with a Network Access Server (NAS).

The Gi interface is used to transmit the following messages:

- AAA Server responds to the following RADIUS requests:
  - Access-Request
  - Accounting-Request (start/stop)
- AAA Server generates the following RADIUS messages:
  - Access-Accept
  - Access- Reject
  - Accounting-Response
  - Disconnect-Request

The AAA Server RADIUS interface is configured with its own virtual IP address and port.

In a WiMAX environment, the AAA server interworks with one or multiple ASN-GWs (Access System Network-Gateways) and Home Agents.

LTE-HSS interfaces

The LTE-HSS is connected to an MME or a SGSN using the Diameter Protocol defined by the IETF in the RFC3588. The under layer transport that is used to connect two diameter peers (LTE-HSS and MME for instance) is TCP or SCTP. The Diameter interface used between the LTE-HSS and the MME is named S6a while S6d is the one used between the LTE-HSS and the SGSN.

The S6a interface enables the transfer of subscription and authentication data for authenticating/authorizing user access to the LTE-HSS between the MME and the LTE-HSS

The S6d interface enables the transfer of subscriber related data between the SGSN and the HSS

The procedures, message parameters and protocol are similar between S6a and S6d. S6a is used for location changes of the MME, while S6d is for location changes of the SGSN.

Through these interfaces, the LTE-HSS supports the following types of messages:

- Update Location Request/Answer (ULR/ULA), Cancel Location Request/Answer (CLR/CLA), Purge UE Request/Answer (PUR/PUA) messages for Location Management procedures
- Delete Subscriber Data Request/Answer (DSR/DSA), Insert Subscriber Data Request/Answer (IDR/IDA) messages for Subscriber Data Handling Procedures
- Reset Subscriber Request/Answer (RSR/RSA) messages for Fault Recovery Procedures.

- NotifyRequest/Answer (NOR/NOA) messages for Notification Procedures.
- Authentication Information Retrieval/Answer (AIR/AIA) for Authentication Procedures.

LTE-EIR interfaces

The LTE-EIR is connected to an MME or SGSN using the Diameter protocol and the S13 or S13' interface:

- The S13 interface enables the ME Identity check procedure between the MME (Mobility Management Entity) and the EIR.
- The S13' interface enables the ME Identity check procedure between the SGSN and the EIR.

Both interfaces use the TCP/SCTP protocol for transferring signalling messages.

SPR interfaces

The 3GPP Diameter Sh Release-10 is the interface implemented by the SPR to communicate with the PCRF . Although the SPR doesn't yet fully support the Sh Release-10, the current level of compliance of the SDM with respect to the Sh interface is sufficient to communicate with the PCRF. For details on the Diameter Sh interface, refer to the previous section.

The PCRFs can query User Profile data and can query or update Quota and State data using Sh transparent data mechanisms. In order to maximize performance on the PCRF-SPR interface, Sh Transparent data is stored by the SPR as a 'blob' (binary large object), however access to specific fields within the user profile 'blob' is provided on the provisioning interfaces.

The SPR allows a PCRF to read/write/subscribe to Transparent Data when using one of the following keys in Sh messages:

- MSISDN
- NAI
- IMSI

The Sh connectivity is based on Diameter/TCP. All SPR and PCRF blades are in the same Diameter realm, but with different hostnames.

A typical scenario is to have one Sh connection between each PCRF and SPR blade. In the case where this main connection fails between a PCRF and a SPR, the PCRF will establish a new connection with another SPR.

As per example, in the case where two sites run the SPR functionality on two blades (see figure below), each SPR blade supports one active Sh connection and upon failure of other Sh connection(s), an SPR blade could additionally support Sh connections from all of the PCRFs (in this case: up to 3 Sh connections).

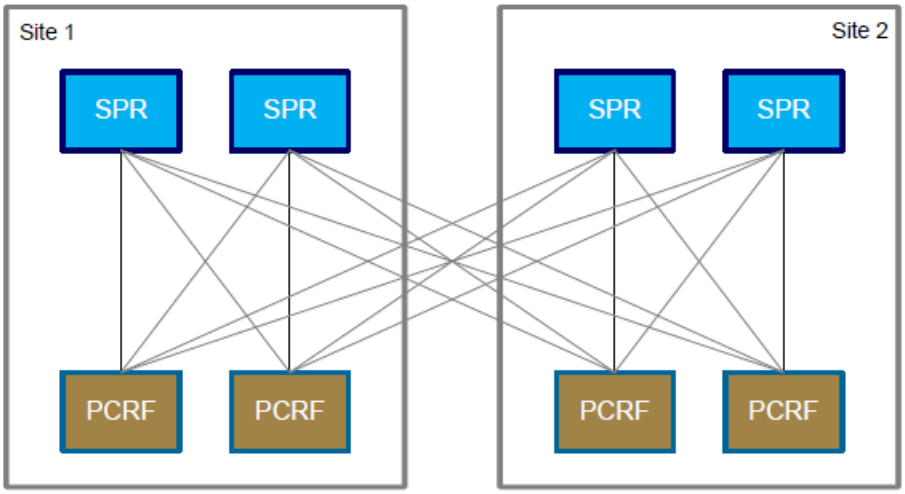


Figure 2: SPR Sh connectivity

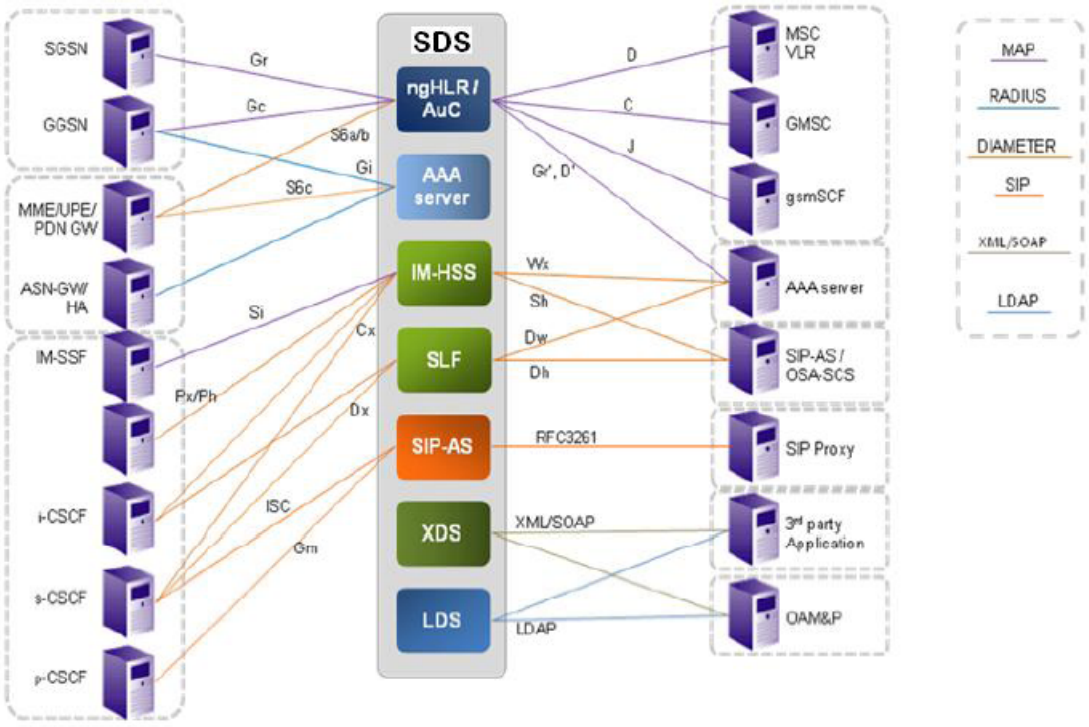
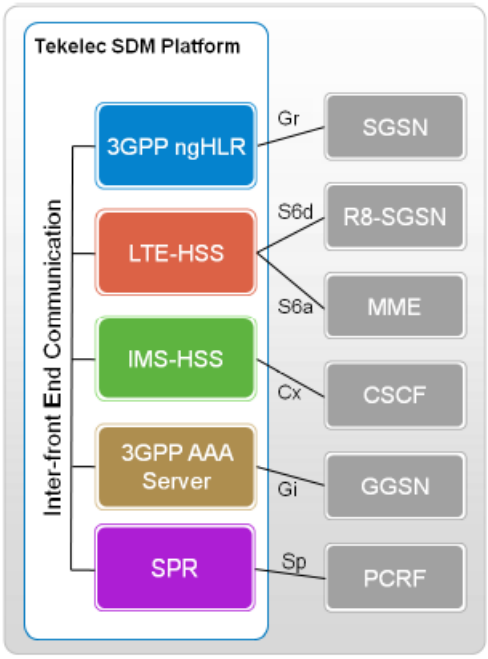


Figure 3: SDM Supported Interfaces

Figure 4: Inter-front-end communication



Protocols

SS7 overview

The Tekelec ngHLR network node communicates with other network entities through signaling system number 7 (SS7). SS7 is a telecommunications protocol defined by the International Telecommunication Union (ITU). The SS7 network and protocol uses out-of-band signaling to support call setup and management, billing, routing, and information exchange functions of the public switched telephone network.

The hardware and software functions of the SS7 protocol are divided into seven functional levels. These levels map loosely to the Open Systems Interconnect (OSI) 7-layer reference model defined by the International Standards Organization (ISO). This model describes the structure for modeling the interconnection and exchange of information between users in a communications system.

The SDM supports the Interphase 3639 and 4539F cards. They offer the possibility to configure some of the ports with the MTP2 layer protocol narrow band Low Speed Link (64 kbps/channel where 1 link can have up to 32 channels) or High Speed Link (1544 kbps/link) and/or with the ATM broadband (1920 kbps/link) using the SAAL protocol to use the most SS7 capacity. The SDM can also use the SIGTRAN feature that integrates the Trillium M3UA and Linux/SCTP stack to send and receive SS7 signals over the IP network.

The following figures show how the SS7 model relates to the OSI model in the three cases where the SS7 uses MTP 1 and 2 layers or where the SS7 uses the Signaling ATM Adaptation Layer (SAAL) or the SCTP/M3UA (SIGTRAN feature).

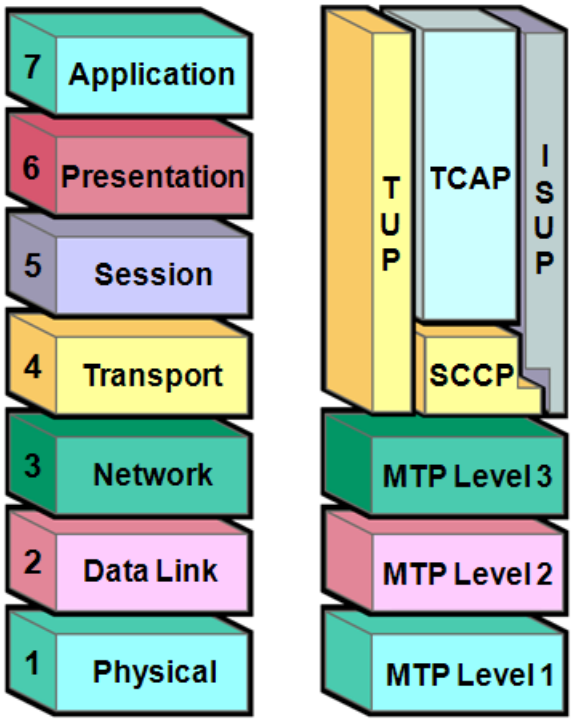


Figure 5: The OSI Reference Model and the SS7 Protocol Stack using MTP 1 and 2 Layers

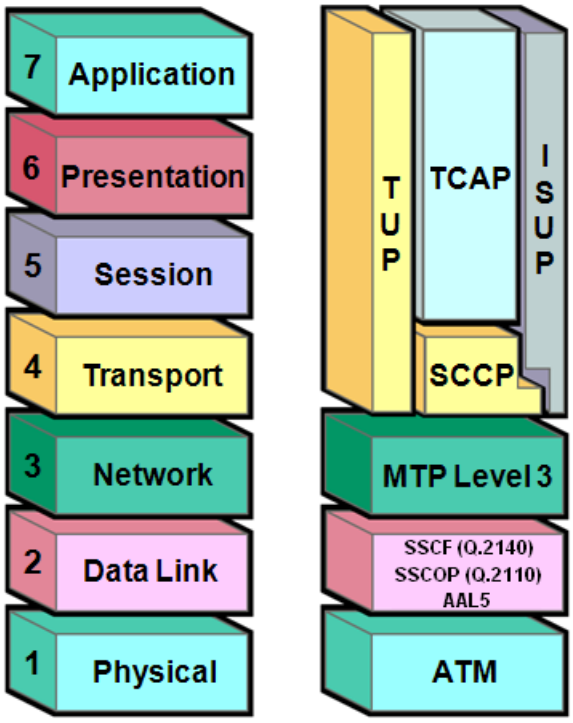


Figure 6: The OSI Reference Model and the SS7 Protocol Stack using SAAL

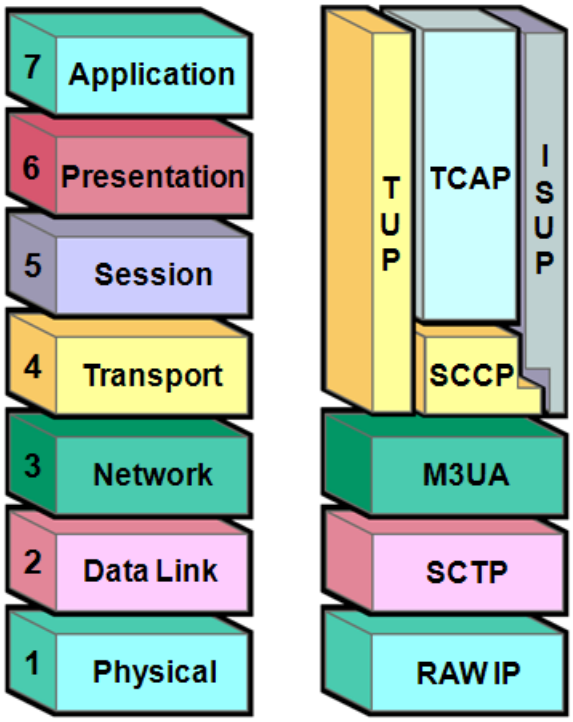


Figure 7: OSI Reference Model and the SIGTRAN Stack using SCTP/M3UA protocols

The lowest three levels of the SS7 architecture, called the Message Transfer Part (MTP), provide a reliable but connectionless (datagram or packet style) service for routing messages through the SS7 network. This service is used by the various user parts described below.

- *MTP 1* represents the physical layer, which is the layer that is responsible for the connection of SS7 Signaling Points into the transmission network over which they communicate with each other. Primarily, this involves the conversion of messaging into electrical signal and the maintenance of the physical links through which these pass. Physical interfaces defined include E-1 (2048 kb/s; 32 64 kb/s channels), DS-1 (1544 kb/s; 24 64kb/s channels), V.35 (64 kb/s), DS-0 (64 kb/s), and DS-0A (56 kb/s).
- *MTP2* represents the signaling link layer. The Tekelec ngHLR uses the Interphase 3639/4539F cards which can be configured using the MTP2 narrow band Low Speed Link or the MTP2 narrow band High Speed Link(as per standard Q.703 - Annexe A). The MTP2 protocol is a narrow band data link control protocol that provides for the reliable sequenced delivery of data across a signaling data link. Level 2 implements flow control, message sequence validation, and error checking. When an error occurs on a signaling link, the message (or set of messages) is retransmitted.
- *SAAL* (signaling ATM Adaptation layer) is a broadband protocol that uses fixed-length 53 octet cells and that can replace the MTP Levels 2 and 1. MTP Level 3 interfaces to ATM using the Signaling ATM Adaptation Layer (SAAL). The MTP1 layer is replaced by the ATM and the MTP2 layer is replaced by the AAL5, SSCOP as per the Q.2110 standard and the SSCF as per the Q.2140 standard.
- *TUCL* (TCP/UDP Convergence Layer) is a generic protocol software layer that provides support for reliable and unreliable transport mechanisms. TUCL is used by the SCTP layer to access to RAW IP/IPv6 services.
- *MTP 3* , also called the signaling network layer, provides for routing data across multiple STPs from control source to control destination. MTP Level 3 re-routes traffic away from failed links and signaling points and controls traffic when congestion occurs.

- SCTP , also called the Stream Control Transmission Protocol. The SCTP association provides the transport for the delivery of M3UA adaptation layer peer messages. This protocol replaces the MTP Levels 2 and 1 when using the SIGTRAN feature. In the SDM system, the SCTP protocol is controlled by the Operating System's kernel, using a Linux/SCTP stack. The M3UA interfaces with the TUCL layer that uses the LKSCTP library to communicate with the Kernel SCTP .
- M3UA (MTP3-User Adaptation Layer) is used for point-to-point signaling between two IP Server Processes (IPSPs) when using the SIGTRAN feature. It replaces the MTP3 layer to route and transport data to the SCCP layer via IP. The M3UA layer provides the same set of primitives and services as its upper layer as the MTP3, except it extends access to the MTP3 layer services to a remote IP-based application. The M3UA layer provides the transport of MTP-TRANSFER primitives across an established SCTP association between IPSPs. Information blocks with a Signaling Information Field (SIF) larger than 272 octets can be accommodated directly by M3UA/SCTP, without the need for an upper layer segmentation/re-assembly procedure.
- Signalling Connection Control Part *(SCCP)* , provides connectionless and connection-oriented network services and global title translation (GTT) capabilities above MTP Level 3 and M3UA. A global title is an address (e.g., a dialed 800 number, calling card number, or mobile subscriber identification number) which is translated by SCCP into a destination point code and subsystem number. A subsystem number uniquely identifies an application at the destination signaling point. SCCP is used as the transport layer for TCAP-based services.
- The MTP and the SCCP together form the Network Service Part (NSP). The resulting split in OSI network functions between MTP and SCCP has the advantage that the higher-overhead SCCP services can be used only when required, and the more efficient MTP services can be used in other applications

The remaining parts of the SS7 protocol stack are concerned with the actual contents of the SS7 messages and are sometimes called application layers. These include:

- *ISDN User (ISUP)* provides the signaling needed for basic ISDN circuit-mode bearer services as well as ISDN supplementary services having end-to-end significance. ISUP is the protocol that supports ISDN in the Public Switched Telephone Network. It corresponds to the transport, session, presentation, application layers and part of the network layer of the OSI model.
- *Telephony User Part (TUP)* is an ISUP predecessor in providing telephony signaling functions. TUP has now been obsolete by ISUP in most countries and in the international network. The TUP corresponds to the transport, session, presentation, application layers and part of the network layer of the OSI model.
- Transaction Capabilities Application Part *(TCAP)* provides the mechanisms for transaction-oriented (rather than connection-oriented) applications and functions. The TCAP corresponds to the application layer in the OSI model. TCAP is often used for database access by the SS7 switches but has many other applications through the network.
- Application Service Elements (ASEs) represent user parts that are highly application-specific, for example:
  - Intelligent Network Application Part (INAP)
  - Mobile Application Part (MAP) provides the signaling functions necessary for the mobile capabilities of voice and non-voice applications in a mobile network
  - IS41 is an ANSI signaling standard used in cellular networks

Diameter overview

The HSS and LTE-HSS network nodes communicate with other network entities through the Diameter. Diameter is defined as a client-server protocol. The Diameter Base Protocol is a telecommunication

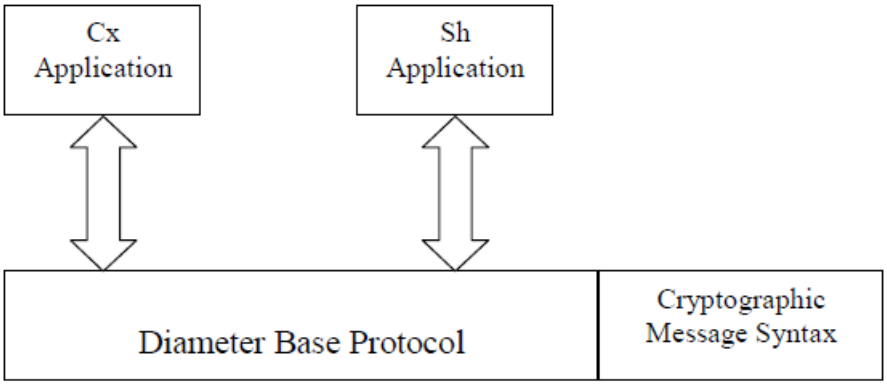
protocol developed by the IETF to enable services such as IP mobility, SIP authentication, and on-line charging and selected by the 3GPP as the standard for Authentication, Authorization, and Accounting functions (AAA).

The Diameter Base Protocol relies on top of different transport protocols, but it is limited to IP networks. The Diameter Base Protocol runs on the default port 3868, modifiable, of either the TCP or SCTP transport protocols. For now, the HSS server supports only TCP, but in future releases of the HSS, SCTP will also be supported.

The Diameter model is a base protocol and a set of applications where the base protocol provides common functionalities to the supported applications. The base protocol must, therefore, be used in conjunction with a Diameter application, which for the HSS can be the Cx and Sh applications. These applications rely on the services of the base protocol to support a specific type of network access.

Applications are defined as extensions on the Diameter base protocol. Each application inherits the functionality and AVPs of the base protocol. The Diameter sessions are established as point-to-point terminated sessions between the HSS/LTE-HSS and the Diameter peers, which can be a CSCF or an Application Server. These sessions are implicitly terminated, meaning that the HSS Diameter Server does not have to maintain the state information for these sessions. The figure below depicts the Diameter's architecture.

Figure 8: Structure of Diameter Base Protocol



The Diameter Base Protocol is a transport protocol which

- is very extensible,
- is not dedicated to a particular application,
- is suitable to carry user-related information,
- provides useful default state machines for authentication and accounting, and
- provides a useful routing and network deployment framework for authentication and accounting.

The base protocol defines the basic Diameter message format. Data is carried within a Diameter message as a collection of Attribute Value Pairs (AVPs). An AVP consists of multiple fields: An AVP Code, Length, Flags and Data. Some AVPs are used by the Diameter base protocol; other AVPs are intended for the Diameter applications as depicted in the figure above. A Diameter message consists of a fixed-length 20 octet header followed by a variable number of AVPs.

The Diameter Cryptographic Message (CMS) application provides end-to-end authentication, integrity, confidentiality and non-repudiation at the AVP level. Individual AVPs may be digitally signed or encrypted.

It is important to differentiate the Cx/Dx and Sh/Dh applications from Diameter, where Diameter is just a base protocol, a "Framework" to transport some user-related information, whereas Cx/Dx and Sh/Dh are "Diameter Applications" defined by 3GPP, on top of the Diameter base protocol.

Both the Base protocol and the Diameter Applications are defining AVPs and Command Codes. Moreover, additional AVPs are defined by 3GPP for each diameter application, using the Diameter Base Protocol. The Base protocol also defines data format, which is a collection of AVPs.

RADIUS overview

The AAA Server (part of the HSS Service) communicates with other network nodes using the RADIUS protocol. The RADIUS protocol is a client-server protocol developed by the IETF and is used for Authentication, Authorization, and Accounting functionality in IP networks by both the IETF and the 3GPP.

The AAA Server makes use of RADIUS over IPv4 UDP connections. The AAA Server is configured with a virtual IP address and port to use for the RADIUS interface.

When used in non-3GPP networks, the RADIUS protocol is used as specified in RFCs 2865, 2866 and 3576. Users are identified using a username/password combination and the network is specified using either a Called-Station-Id or a realm.

When used in a 3GPP network, the RADIUS protocol is used for interworking with a GGSN as specified in TS 29.061. In this context, the GGSN will specify the Access Point Name (APN) via the attribute Called-Station-Id, and may also provide additional user information, such as MSISDN, using attribute Calling-Station-Id. 3GPP TS 29.061 specifies how additional 3GPP attributes are mapped to the RFC defined attributes.

RADIUS is typically used to control users trying to access a network. A user provides credentials (username / password) to a Network Access Server (NAS) using a link-specific protocol. The NAS uses the RADIUS Access-Request message to send the user credentials to a RADIUS server, using authentication schemes PAP or CHAP. When authenticated, the RADIUS server responds with Access-Accept, which also provides information on what network services are authorized. As part of the authorization, the RADIUS server also provides an IP address for the user. While the user remains connected to the network, the NAS will periodically issue Accounting-Request messages to the RADIUS server, which keeps track of the user's usage of network resources. When the user disconnects from the network, an Accounting-Request Stop message is issued by the NAS to indicate the session has terminated and resources are freed.

Chapter 3

Software description

Topics:

This chapter describes the software architecture, system and subscriber management, and application features.

Software architecture

The figure shows a high level view of the SDM software architecture.

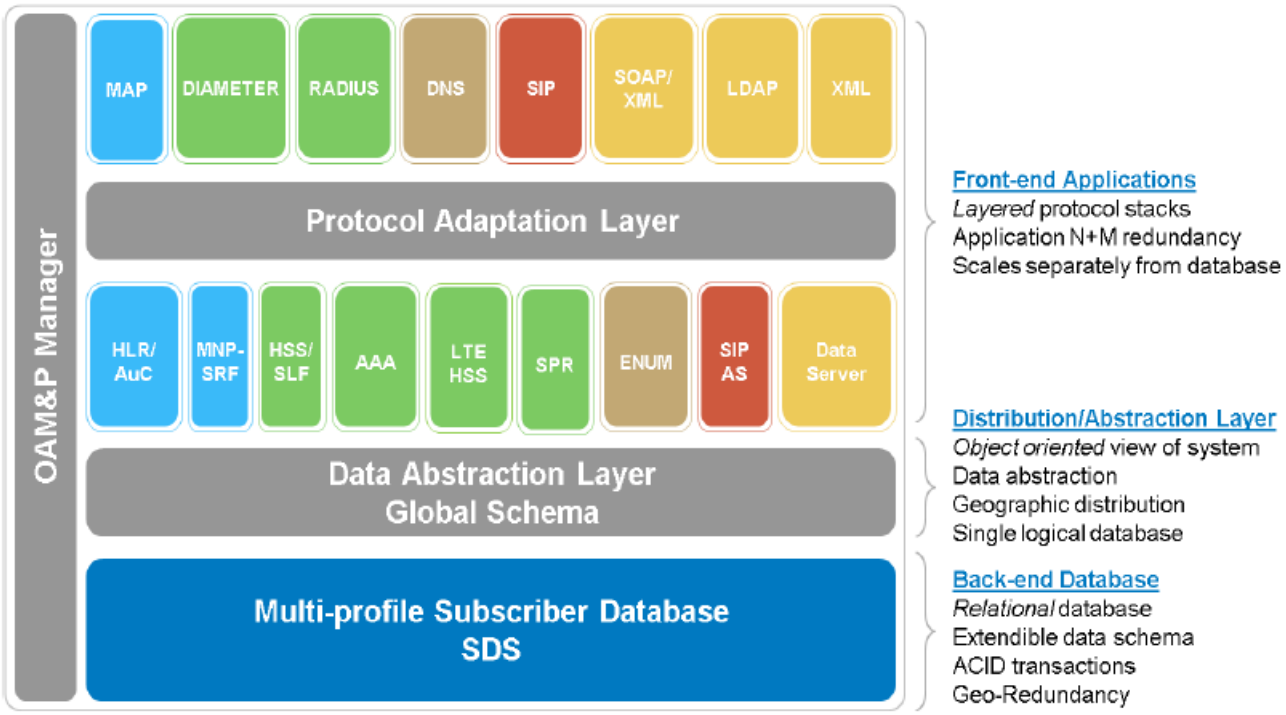


Figure 9: SDM high level software architecture

The system can be composed of up to 2 slots for rackmount Single Board Computers (SBC), and up to 16 slots for blade SBCs. This means that up to two or sixteen slots can have assigned SBCs that offer services.

Note: The number of HP server/storage blades supported depends on the configuration of the system.

Services Running on the System

This section describes the following:

- The identities that can be bound to each slot
- The core/user services and their modules that can run on the system
- The high-availability states of the services
- The high-availability mechanisms

To provision a slot, an identity must be assigned to it. An identity defines the basic set of services that run on the blade. These basic set of services are core, backend, and framework services.

Two identities exist:

Table 2: Identities and their services

Identities	Services
System Controller	Core service: CoreSystemController
	Backend service: Database
	Framework service: DataAccess
FrontEndNode	Core service: CoreServiceNode

These identities determine the basic software services running on a blade. Typically, there are two System Controller nodes (SC blades) (i.e., each bound to the SystemController identity) and additional front-end nodes (FE SBCs) (i.e., each bound to the FrontEndNode identity). Front-end nodes do not have a local copy of the database.

Binding Services

The system also allows binding User Services to a slot. The User Services are:

- Hlr service (in which the HlrServer module includes the SIP functionalities)
- Hss service (which can include the SLF and AAA Server functionalities)
- LteHss service
- Ldap service
- Ras service

A service is composed of a set of modules (processes) that participate together in offering a specific service. Each service binding to a slot is represented by a ServiceInstance entity.

Services bound to a slot define the set of modules that start on that slot. There are various services to fit the different applications offered by Tekelec. A given service regroups mandatory and optional modules that are defined as a ModuleType. A module can be excluded from the service. Some of these Module Types are also subject to licenses.

The system supports these services with their associated module types:

Table 3: Services and their module types

Service	Service Type	Module Type
CoreSystemController	Core	NodeManager
		OampEventMgr
		OampManager
		OampPerformanceManager
CoreServiceNode	Core	NodeManager
Database	Backend	DpController
DataAccess	Framework	XmlDataServer
		DataAccessServer
Hlr	User	HlrServer

Hss	User	HssServer
LteHss	User	LteHssServer
Ldap	User	LdapDataServer
Ras	User	RasServer

Service Types

Services are separated into categories set by the ServiceType attribute:

- *Core Service:* A core service is a service that is defined by the Identity bound to a slot. Core service provides the basic infrastructures required to add applications on a blade. The operator cannot add or remove a core service explicitly from a slot. Core services are added and removed implicitly by adding or removing an identity.
- *Backend Service:* Backend service provide database infrastructure used by applications. Backend services are automatically added when binding a proper identity to a slot. Operator cannot add or remove manually backend service. Take note that n o service can run on a blade if a backend service is not in service on that blade.
- *Framework Service:* Framework services provide system basic and critical configuration services. Those kind of service are automatically added on System Controller node but can be optionally added by the operator on FrontEnd blade. Framework service should not be removed from System Controller node.
- *User Service:* A user service contained modules that implement an application that provides telecommunication services to subscribers. A user service is a service that an operator can add to a slot or remove from a slot. The only requirement to add or remove a service is that an identity must first be bound to the slot.

High-availability service states

The instances of each service are highly available. Each service instance has four states to describe its High-availability state:

- HaRole (high-availability role)
- OpState (operational state)
- AdminState (administrative state)
- ResourceState

Each service type is also known as a service group since they each regroup multiple instances. Up to one instance of a service group can run on a blade and multiple instances of different service groups can run on a blade.

Operational state and HA role

The instances of each service are highly available. Each service instance has four states to describe its high-availability state:

- HaRole (high-availability role. The HA role has three values:
  - Unassigned - all instances that are not active nor standby. These are usually slave instances that refer to the active instance.
  - Active - the active instance is the master instance

  - Standby - the standby instance that represents the next instance that will become active in case of failure of the active instance.

- OpState (operational state): indicates whether the instance is operational (provides service) or unoperational (doesn't provide service). It can take two values:
  - Enabled - the instance provides service
  - Disabled - the instance does not provides service

The system supports the following OpState and HaRole combinations:

- Disabled-Unassigned
- Enabled-Active
- Enabled-Standby
- Enabled-Unassigned
- Enabled-Unassigned

The OpState is used to indicate if the module is providing service or not. The HaRole is used to give the role of the instance within its service group. The active role is used to identify the master or reference of the service group. The standby represents the next active instance in case of failure of the current active. The unassigned role, if the opState is enabled, indicates that the instance's modules are providing service but is taking the slave or replica role. Therefore, this means that the HaRole is not used to indicate if a service is in-service or out-of-service. All service groups support a maximum of 1 active and 1 standby since the system has no need for dual master or reference.

Administrative state

The administrative state (AdminState) is used to lock or unlock a module. When a module is locked, the module and its dependents' OpState transition to disabled. If the HaRole of a module is active or standby and the module is locked, the HaRole will transition to unassigned.

Administrative locking is used to keep the database component disabled until the database is synchronized. It is also used for the System Controller to initiate a manual switchover.

Resource state

The resource state is used to indicate the status of a process. There are 5 values possible:

- NoResource
- PoweredOff
- Uninitialized
- Healthy
- Failed

The noResource state means that the process is not started or not registered to the internal process that manages the services and there are no available resources to provide service. The healthy state means that the process is started and successfully managed internally. The failed state means that the process has failed. The *uninitialized* state means that the module is currently being initialized. The *poweredOff* state means that the module is in the process of being *shut down*.

High availability mechanisms

Three main redundancy models ensure high-availability of the services:

- Active/Standby (1+1) redundancy model
- Active/Unassigned (1+N) redundancy model
- Active/Standby/Unassigned (1+1+N) redundancy model

Each service group follows one of these redundancy models.

The model type specifies the number of active module, standby and unassigned modules.

In a 1+1 redundancy model, there is one active instance and one standby instance and there is a threshold of one (minimum number of active service instances needed to continue to provide services). In this model:

- The standby instance does not provide service, it only takes over when the active instance fails.
- The active and standby instances both run on the System Controller blades.

In a 1+N redundancy model, there is one active instance and N unassigned instances and a threshold of one (minimum number of active service instances needed to continue to provide services). In this model:

- All the instances provide service granted of course that they all are enabled (OpState). The location of the next active instance is unknown.
- The unassigned instances all refer to the active one and in case of failure of an instance, the instances that remain enabled take on the load of the failed instance in addition to their already assigned load. In case of failure of the current active instance, one of the unassigned-enabled node becomes the new active one.

In a 1+1+N redundancy model, there is one active instance, one standby instance and N unassigned instances and a threshold of one (minimum number of active service instances needed to continue to provide services). In this model:

- All the instances provide service (even the standby one) granted of course that they all are enabled (OpState). The standby state serves only to identify the next active instance in case of failure of the current active instance.
- The unassigned instances all refer to the active one and in case of failure of an instance, the instances that remain enabled take on the load of the failed instance in addition to their already assigned load. In case of failure of the current active instance, the standby instance becomes the new active one.

The table hereby presents a general guideline of all the different services supported by the system with their redundancy model and their general slot location.

Important: The number of instances that can be supported by the system depends on many factors, such as the type of configuration setup for the SDM system (applications and functionalities enabled), the Operator's network configuration, the number of transactions per seconds (TPS) going through the system, etc. Please contact Tekelec's SDM Customer Support for a more specific and customized configuration of the SDM system as per your needs.

Table 4: Services redundancy model and location guidelines

Service	Redundancy model	Slot Location
Hlr	1+1+N	2-4 blade systems: 1 instance per blade (SystemController (SC) and FrontEnd (FE)) blade. 8-16 blade systems: 1 instance per FrontEnd blade. No instance on SC blades.
Hss	1+N	2-4 blade systems: 1 instance per System Controller blade (1 in active state, 1 in unassigned state, both providing service). 8-16 blade systems: 1 instance per FrontEnd blade. No instance on SC blades.
LteHss	1+N	2-4 blade systems: 1 instance per System Controller blade (1 in active state, 1 in unassigned state, both providing service). 8-16 blade systems: 1 instance per FrontEnd blade. No instance on SC blades.
CoreSystem Controller	1+1	1 instance per System Controller blade.
CoreService Node	1+N	1 instance per FrontEnd blades.
Database	1+1+N	The active and standby instances must run on the System Controller blades. The active instance running on the SC blade is the only one that provides the service of writing into the database. It is the reference database. The standby instance is a replica, but is ready to take on the reference role upon failure of the active instance.
DataAccess	1+N	1 instance per blade.
Ldap	1+1	1 instance per System Controller blade.
Ras	1+N	1e instance per blade.

Note:

All services have a dependency with the *Database* service group.

The figure represents the provisioned slots for a four-blade system. For the two blade system, only the SC blades are supported and the active instances are on one of those blades. For the eight and sixteen blade system, it follows the same logic but with more FrontEnd blades.

Important:

- The number of instances that can be supported by the system depends on many factors, such as the type of configuration setup for the SDM system (applications and functionalities enabled), the Operator's network configuration, the number of transactions per seconds (TPS) going through

the system, etc. Contact the *Customer Care Center* for a more specific and customized configuration of the SDM system as per your needs.

- On a two- and four-blade system, User Services can run on the same blades as a Core System Controller service. However, for the eight- and sixteen-blades system, no User Service can run on the same blade as the Core System Controller service. For example, on an eight-blade system, up to six instances of the Hlr service can be provisioned on the slots bound with the CoreServiceNode service. Following the same logic, up to ten instances of the Hlr service can be provisioned on the slots bound with the CoreServiceNode.

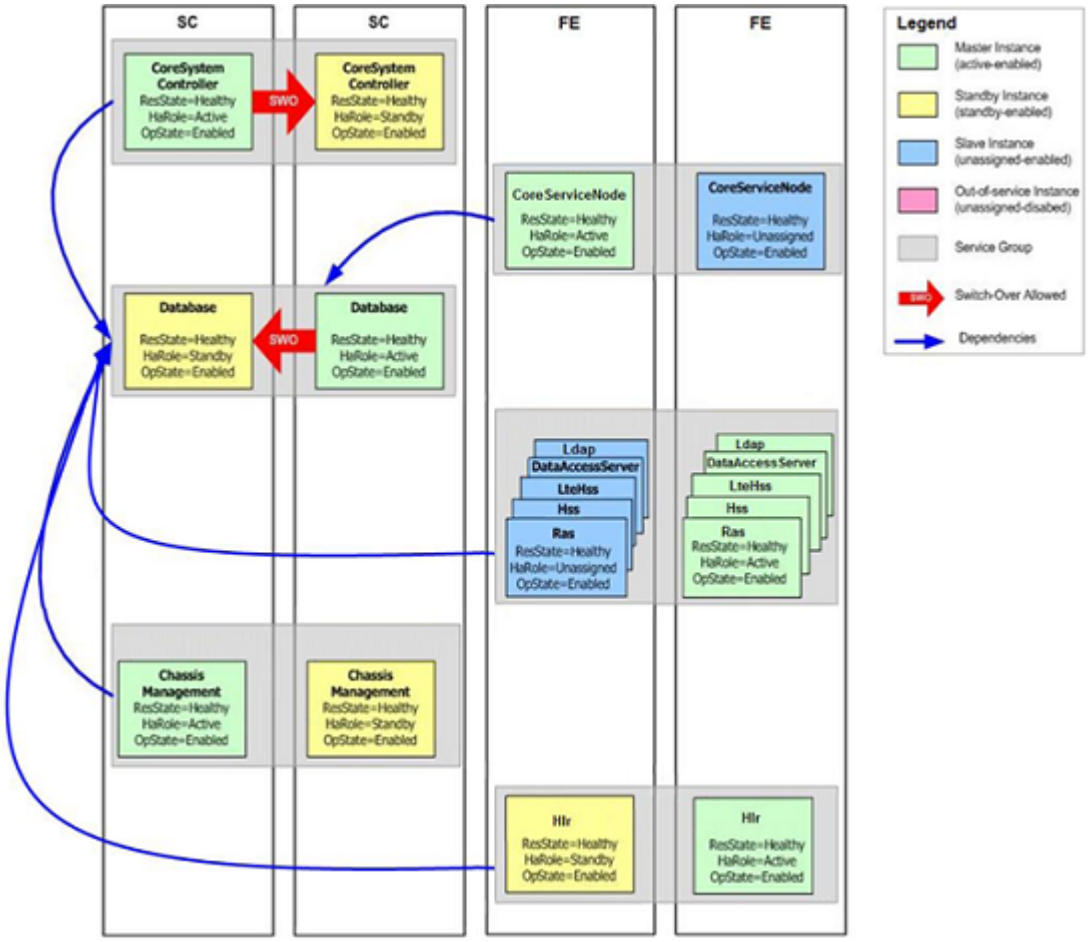


Figure 10: Services on four-blade system

Applications and functionalities supported by the SDM

The SDM solution offers the support of the following front-end applications, which can all run over the Subscriber Data Server back-end application, on one single hardware platform:

- 3GPP ngHLR (SIP-AS)
- Next Generation Number Portability
  - ENUM
  - SIP-NP

    - MNP-SRF
- IMS-HSS
- LTE-HSS
    - LTE-EIR
- 3GPP AAA
- SPR
- EIR

The following sections present a more detailed description of the main processes that handle/manage the functionalities supported by the SDM's applications:

- *HLR Server*
- *HLR Provisioning Manager*
- *SS7 Manager*
- *AuC Server*
- *SIP Server*
- *SIP Provisioning*
- *GSM Registration Agent*
- *HSS Server*
- *HSS Provisioning Manager*
- *HSS authentication center*
- *Policy Provisioning Manager*
- *LTE-HSS*
- *Equipment Identity Register (EIR)*
- *LTE Equipment Identity Register*
- *Ras Server*
- *System Controller*
- *Database*
- *Global Schema*

HLR Server

The main functions of the HLR (Home Location Register) Server are the traditional 2G and 2.5G network services offered by the HLR node, such as centralized mobile subscriber database, location updates, and call handling.

The HLR Server module (process) associated to the HLR Service includes the AuC (Authentication) functionality as well as the SS7 Server and all of its layers (MTP2, SAAL, MTP3, SCCP, TCAP, MAP, SIGTRAN).The HLR Server module interfaces with the OAM&P manager allowing the operator to dynamically configure the SS7 layers and the HLR functionalities. It also interfaces with the database in order to retrieve permanent subscriber data entered by the operator during subscriber provisioning. Any changes of services for a registered subscriber will be identified by the HLR Server and the network will be notified appropriately.

The HLR Server runs on the SBCs (Single Board Computers). Multiple instances of the HLR Server (up to one per SBC blade or in the case where the HLR Server also runs the SIP application: up to 4 instances) can run on each of the SBC blades in an active/standby/unassigned (1+1+N) state, following the 1+1+N redundancy model. This means that there is one active instance, one standby instance and

N unassigned instances of the Hlr service that run simultaneously on the system. Moreover, a threshold of one instance can run on the system in order to provide service (minimum number of active service instances needed to continue to provide services). In this model, all the instances provide service (even the standby one) granted of course that they all are enabled (OpState). The standby state serves only to identify the next active instance in case of failure of the current active instance. As for the unassigned instances, they all refer to the active instance.

In a two and four blade system, an instance of the Hlr service can run on the blade on which the System Controller runs; however, in an eight and sixteen blade system, an instance of the Hlr service should run on a blade provisioned with the FrontEnd identity and shouldn't run on the blade on which the System Controller runs.

All of the Hlr Service's instances run in a load sharing mode (i.e. pure distributed and non-fault tolerant). If the Hlr Server module (process) fails on an instance of the Hlr service, the whole service fails on that blade, the Hlr service instance becomes disabled and the load is redistributed among the remaining active Hlr service instances on the other blades. In such case, no loss of service is perceived by the subscriber. In case of failure of the current active instance, the standby instance becomes the new active one. Please see section *HLR Server* for more details on scalability.

The HLR functional entity is a database in charge of the management of mobile subscribers. A PLMN (Public Land Mobile Network) may contain one or several HLRs: depending on the number of mobile subscribers, on the capacity of the equipment, and on the organization of the network.

The Tekelec ngHLR stores the following information:

- subscription information;
- location information enabling the charging and routing of calls towards the MSC where the MS is registered (e.g. the MS Roaming Number, the VLR Number, the MSC Number, the Local MS Identity);

and, if GPRS is supported:

- location information enabling the charging and routing of messages in the SGSN where the MS is currently registered (e.g. the SGSN Number);

Different types of identity are attached to each mobile subscription and are stored in the HLR. The following identities are stored:

- International Mobile Station Identity (IMSI)
- Mobile Station International ISDN number(s) (MSISDN)

if GPRS is supported, the following information is also stored:

- zero or more Packet Data Protocol (PDP) address(es)

There is always at least one identity, apart from the IMSI, attached to each mobile subscription and stored in the HLR.

The IMSI or the MSISDN may be used as a key to access the information in the database for a mobile subscription.

The database contains other information such as:

- teleservices and bearer services subscription information
- service restrictions (e.g. roaming limitation)
- supplementary services, the HLR contains the parameters attached to these services

if GPRS is supported, it also contains:

- information on whether or not a GGSN is allowed to dynamically allocate PDP addresses for a subscriber.

Note: Not all the supplementary services parameters need to be stored in the HLR. However, it is safer to store all subscription parameters in the HLR even when some are stored in a subscriber card.

HLR Provisioning Manager

The HLR Provisioning Manager (HPM) is a module (process) associated to the DataAccess service and therefore runs on the Single Board Computers (SBCs) in an active/unassigned (1+N) mode. It is used to validate subscriber data entered into the database by the operator. One of its main functions is to verify the consistency of new data entered in the database with existing data. Some services are mutually exclusive and others require previously configured information.

The actual field validation like acceptable ranges, type checking, etc. is done by the OAM&P Manager at a generic level based on the global schema.

Inherent validation at the relational database level is also performed for deletion and creation of records.

SS7 Manager

The SS7 Protocol is used to establish communication between traditional 2G and 2.5G network entities in mobile telecommunication networks. In the SDM implementation, it is divided in three portions.

The MTP1 and part of MTP2 layers run in the firmware of dedicated SS7 hardware cards installed in the PMC mezzanines of the SBCs. An MTP2 convergence layer is used as an adapter allowing the MTP3 layer to communicate with the MTP2 firmware through hardware drivers.

The SDM can support the MTP2 narrowband protocol with Low Speed Links (LSL) or High Speed Link (HSL). By replacing the 16 links of a MTP2 linkset with HSLs, the HLR SS7 capacity gets multiplied by a factor of 20, bringing the total SS7 capacity to over 5 million subscribers (with one linkset).

As another option, the Tekelec ngHLR can also support the broadband ATM by allowing to use the Signalling ATM Adaptation layer (SAAL) protocol in place of the MTP Layers 1 and 2. In this case, the physical and data links layers use Asynchronous Transfer Mode (ATM). The SAAL also runs in the firmware of dedicated SS7 hardware cards installed in the PMC mezzanines of the SBCs. The PMCs of the SDM can support up to four ATM broadband links per card.

When using the MTP2 High Speed Links or the SAAL protocol, the entire bandwidth of a T1/E1 is utilized for the transport of SS7 signaling messages.

The SDM can support for the MTP2 layer (with narrowband LSL or HSL) and/or SAAL to be running on an SS7 card, on which the ports of the card need to be configured accordingly at installation. On a port configured with the MTP2 layer, either low speed links can be created or only one high speed link.

Once the ports of the SS7 card have been configured properly, the operator can configure the SS7 routes, links and all the parameters necessary for SS7 provisioning of the Tekelec ngHLR through the WebCI or CLI. For more information on the SS7 provisioning parameters and the tables that need to be configured, please refer to the "SS7" chapter of the SDM System Configuration - Reference Manual . For step-by-step instructions on how to configure and provision the Tekelec ngHLR with the SS7 protocol, please refer to the "Configuring the SS7 stack using MTP2/SAAL, MTP3 protocols" and "Configuring the SS7 stack using the TUCL/SCTP & M3UA protocols (SIGTRAN)" of the *SDM System Configuration - User Guide*.

As a third option, the Tekelec ngHLR can also support the SIGTRAN feature by allowing to use the MTP3-User Adaptation layer (M3UA) as per RFC4666 and the Stream Control Transmission Protocol (SCTP) as a Linux/SCTP stack within the Operating System's kernel (per RFC2960) in place of the MTP Layers 1, 2 and 3 to transport data via IP. In a SDM system with the SIGTRAN feature enabled, the Hlr service can run IP-based SS7 traffic using the TUCL, SCTP and M3UA protocols. As recommended, two instances of the Hlr service on FrontEnd blades can run a SCTP protocol instance. Each of these two blades has an IP connection with the remote host (i.e., VLR) through the Switch of the system. If an IP connection is lost on one of the two blades, then the other blade can continue running and can take on all the traffic through its IP connection. Note that even if there is only two instances of Sigtran, the system can still distribute traffic over up to 10 Hlr services.

When using the SIGTRAN feature, the transport of SS7 signaling messages is done over 10bT/100bT/1000bT Ethernet Physical interfaces.

In the case where the SIGTRAN feature is enabled, an IP Gateway must be configured on the Tekelec ngHLR to provide primary IP interface to the system. It provides a termination point for Raw IP - SCTP based connections and uses distribution functions to route the SS7 traffic to the active HLR services with the SIGTRAN feature enabled.

For more information on the parameters to configure in order to use the SIGTRAN feature, please refer to the "SS7" section of the SDM System Configuration - Reference Manual and for step-by-step instructions on how to configure the system for the SIGTRAN feature, refer to the "Configuring the SS7 stack using the TUCL/SCTP & M3UA protocols (SIGTRAN)" section of the *SDM System Configuration - User Guide* .

Finally, the SDM can run SS7 traffic through T1/E1 connections using the MTP2 narrowband Low Speed Link or High Speed Link protocol and/or the SAAL protocol both also using the MTP Level 3. Moreover, the SDM can run SS7 traffic through an Ethernet connection (IP) using the TUCL, SCTP and M3UA protocols.

The signaling system (SS7) Stack and all of its layers (MTP2/SAAL, MTP3, SCCP, TCAP, MAP), as well as the SIGTRAN Stack (TUCL, SCTP, M3UA protocols), are integrated within the HLR Server Module (process) of the HLR service, discussed in section *SS7 Manager* module interfaces with the OAM&P manager allowing the operator to dynamically configure the SS7 stack layers.

The following characterizes the SS7 and SIGTRAN Stack and the way they function in the SDM system:

The Stack Manager (SM) and System Manager (SG) components both are in charge of controlling and managing the different SS7 and SIGTRAN layers. These two components are fault-tolerant; the SG is in pure fault-tolerant (active/standby) configuration and the SM is in asymmetric dedicated fault-tolerant (master/slave) configuration. Both master and slave SM have the same system configuration knowledge (i.e.SS7 configuration stored in the SDM Database) and functionality but only the master SM can manage (control) the protocol stack.

The SG is configured in all HLR Server instances, but only 2 instances of the SG are designated as active/standby. The active SG instance controls the SS7 protocol layers resided on all the blades and the standby SG instance is a replica. This means that vital information is constantly replicated to the hot standby instance and in case of failure of the active side, the standby side is ready to take over. The Hlr elects the active/standby SG instances based on the active/standby Hlr instances. In other words, the active SG instance always runs within the active Hlr instance while the standby SG instance always runs within the standby Hlr service instance.

The MTP2/SAAL/TUCL and MAP protocols all run in an N-active conventional mode. Presently on the system, two HLR Service instances (on FrontEnd blades) both run actively an instance of each of these protocols. However, these protocols run in a conventional mode, which means that if one of

these protocol's instance goes down, no standby will take over. The instance running that HLR service will go down and traffic will be re-routed on remaining instances of the HLR service.

The MTP3, M3UA, SCCP, TCAP all run in an N-active distributed mode. This means that for each active HLR Service (from two to ten), an instance of these protocols runs actively. When one of its active instances goes down, the traffic load going through that instance is redistributed and shared with the remaining active instances.

Distributed stacks, such as the MTP3, M3UA, SCCP and TCAP stacks, must each have one instance defined as Master. Every instance of these stacks run on each blade as Master or Shadow and are configured identically. The instance defined as the Master is the one from where all control operations are executed and it is responsible to distribute the resulting effect and information to all of its Shadow instances. In a sixteen blade system, ten Hlr services can run traffic and so ten instances of the MTP3, M3UA, SCCP and TCAP stack run traffic with one of each defined as Master and the nine other instances defined as Shadow.

Once the SS7 messages reach the MTP2/SAAL layer, they are sent to the local active MTP3/M3UA instance.

At the top of MTP3 and M3UA level, the Lower Load Distributed Function (LLDF) SCCP performs a load distribution in a round-robin manner based on a dynamic distribution algorithm in order to distribute SS7 traffic to various active SCCP instances located on different blades.

This load distribution takes effect on all the SS7 instances running on the superior layers, which means that the MAP and HLR also end up working in an N-active distributed mode.

In sum, on a SDM system, only the MTP2/SAAL/TUCL protocols run in an N-active conventional mode.

In the case of a new transaction initiated by the VLR (Update Location Request), the LLDF TCAP will send directly the SS7 messages to local TCAP layer.

In the case of an open transaction from the HLR (i.e. when the VLR sends an ISD acknowledgement message to the HLR), the LLDF TCAP will redirect the SS7 messages to the active TCAP instance running on the same blade as the HLR that originally initiated the dialogue. Finally, once the TCAP receives the SS7 messages, it'll process them and send them to the local MAP layer, which in turn, forwards them to the local HLR

The figures below give a representation of the SS7 layers within the HLR Service provisioned on each slot of the system, firstly for a two blade system and secondly for a four blade system.

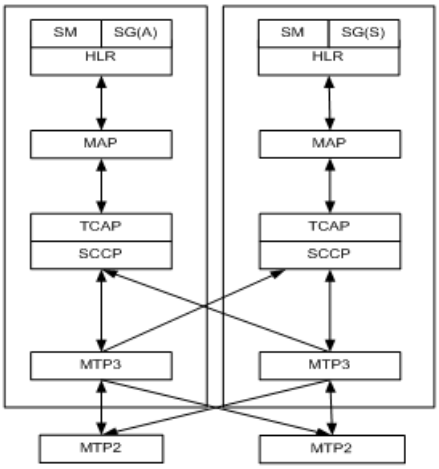


Figure 11: Scalability of SS7 layers within the Hlr service for a two blade system

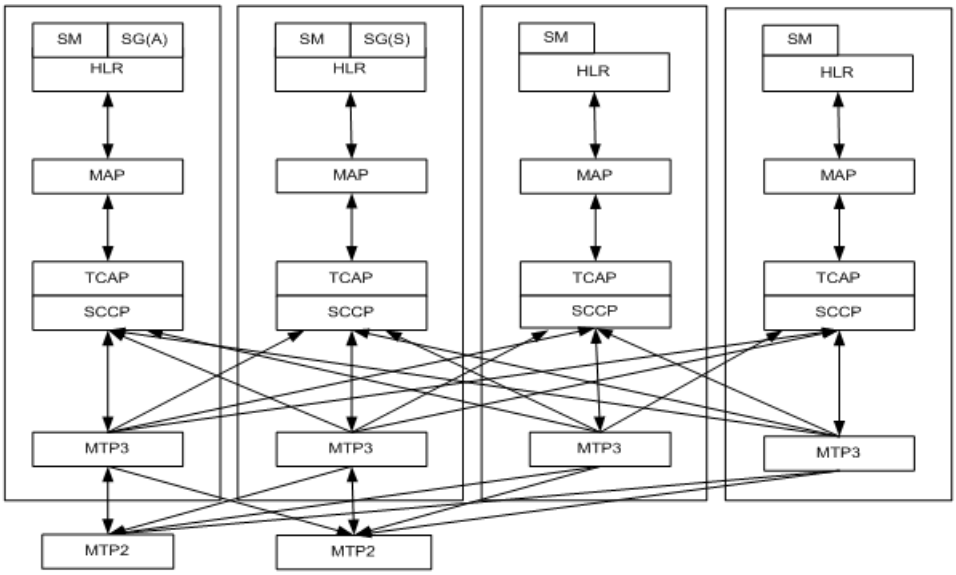


Figure 12: Scalability of SS7 layers within the Hlr service for a four blade system

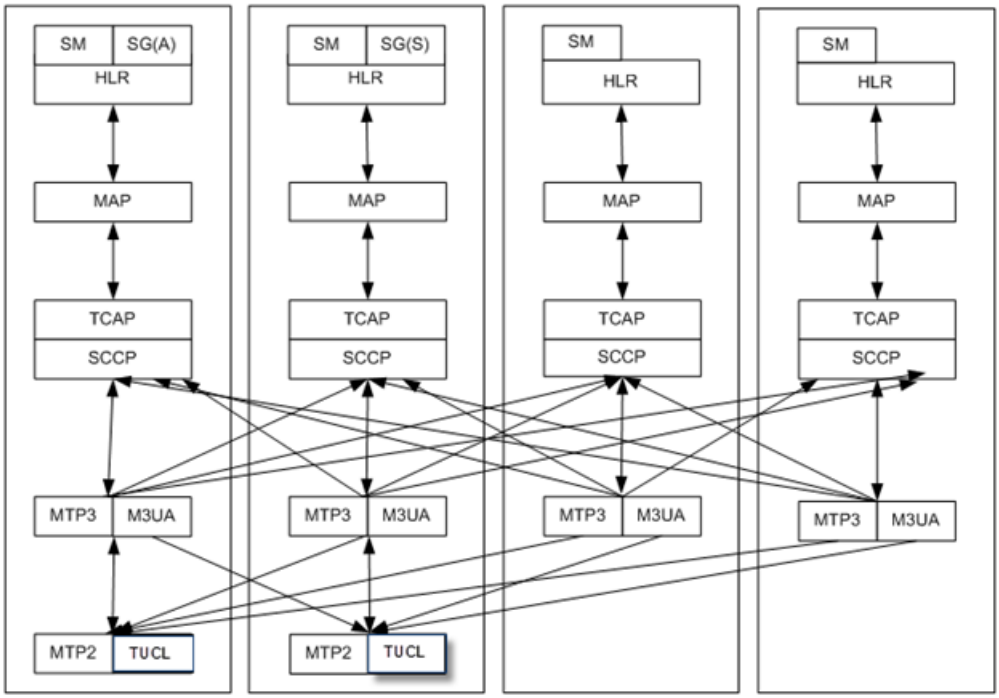


Figure 13: Scalability of SS7 and SIGTRAN layers within the HLR Service for a four blade system

AuC Server

The Authentication Center provides authentication and radio link privacy to users on the GSM network. The Authentication Center supports XOR and GSM Milenage algorithms. Optional support can be provided for COMP128, COMP128-2, and COMP128-3. The Authentication Center (AuC) is integrated into the HLR Server module (process), which is associated to the HLR Service. It interfaces with the telecommunication network through the corresponding HLR messages as defined in the 3GPP MAP specifications. The AuC supports segmentation at the MAP level.

The HLR Service runs in an active/standby/unassigned (1+1+N) mode. This means that there can be multiple instances of the HLR Service, all running traffic. With an AuC Server being integrated in each HLR Service instance, we can say that the AuC Server also operates in an active/standby/unassigned (1+1+N) mode. In the case of failure of a HLR Service instance, the traffic load of that instance will be redistributed throughout all the other active HLR Service instances. Please refer to section for more information on the Hlr service's redundant mode.

SIP Server

The SIP Server application provides the Tekelec ngHLR with the functional SIP Registrar, SIP location service entities, Gsm Registration Agent (SIP User Agent Client) as well as with the SIP Redirect Server as defined in RFC 3261. The SIP Server plays different roles depending on the deployment model used by the operator.

In order to achieve the appropriate functional behavior that is desired for the network, the SIP Functional components of the Tekelec ngHLR's SIP Server can be enabled or disabled individually.

The SIP Registrar processes incoming SIP requests and updates the Tekelec ngHLR database with the contact information from the Register message.

The SIP Redirect function provides redirect capabilities. In response to a SIP Invite request, the Redirect Server interacts with the Registrar's database of registered contacts and with the HLR Server to retrieve all contact information, which is then returned in a SIP Redirect Response. The messaging between SIP Redirect and HLR Server is internal to the Tekelec ngHLR.

The Gsm Registration Agent function (SIP User Agent Client) registers Tekelec ngHLR subscribers with an external SIP Registrar. The Gsm Registration Agent (GRA) performs a SIP Register (or deregister) as per RFC 3261, based on the subscriber's GSM registration state. The HLR Server interacts with the GRA and sends it a message when a SIP Register or deregister is needed. The messaging between HLR Server and GRA is internal to the Tekelec ngHLR.

The SIP Server is integrated with the HLR and therefore one single SIP Server instance runs on each of the SBCs (Single Board Computers) within the HLR Server and uses one single SIP Stack and library for all its functionalities: SIP Registrar, SIP Redirect, Gsm Registration Agent and SIP location services. On each blade, an active SIP Server instance runs and shares the same network IP address and port to process incoming and outgoing traffic for all its functionalities. Moreover, both the UDP and TCP protocols are supported.

Up to four instances of the Hlr service can run both the HLR Server and SIP Server (up to one per SBC (Single Board Computers) blade) on the SBC blades in an active/standby/unassigned state.

The HLR Server/SIP Server's instances run in an active/standby/unassigned (1+1+N) mode and in a load sharing mode (i.e. pure distributed and non-fault tolerant). If the HLR Server/SIP Server module (process) fails on an instance of the HLR service, the whole service fails on that blade, the HLR service instance becomes disabled and the load is redistributed among the remaining active HLR service instances on the other blades. In such case, no loss of services is perceived by the subscriber and the capacity of the system remains the same. Please see section for more details on the redundancy mode of the Hlr service.

SIP Provisioning

The Sip Provisioning functionalities are a subcomponent of the Hlr Provisioning Manager module. The SipProvisioningManager is not a separate module. The HlrProvisioningManager module handles all HLR related subscriber provisioning - both GSM based and SIP based.

The SipProvisioningManager (SPM) module runs on the Single Board Computers (SBCs). It is a software application that processes requests for SIP subscriber provisioning. It is used to validate SIP subscriber data entered into the database by the operator and ensure consistency with existing data.

As previously mentioned, the SIP subscriber profiles and contact locations are stored in the Tekelec ngHLR's database which is updated on the active and replicated to the hot standby.

A single instance of the SIP Provisioning Manager runs within the DataAccess service on each of the SBCs, in an active/unassigned (1+N) mode where all enabled instances process requests. In the case of failure of a DataAccess instance, the traffic is redistributed over the remaining enabled instances.

HSS Server

The HSS Server can handle/manage the following applications:

- IMS-HSS
- AAA

- ENUM
- SPR

The HSS Server is the process of the Hss Service which runs on the SBCs (Single Board Computers). One instance of the HSS Server can run on each SBC in an active/unassigned state, following the 1+N redundancy model (contact Tekelec's Customer Support for a plan of the recommended SDM architecture and configuration as per your needs). This means that there is one active instance and N unassigned instances of the Hss service that run simultaneously on the system. Moreover, a threshold of one instance can run on the system in order to provide service (minimum number of active service instances needed to continue to provide services). In this model, all the instances provide service granted of course that they all are enabled (OpState). The unassigned instances all refer to the active instance.

In a two and four SBC system, an instance of the Hss service can run on the SBC on which the System Controller runs; however, in an eight, twelve or sixteen SBC system, an instance of the Hss service should run on an SBC provisioned with the FrontEnd identity and shouldn't run on the blade on which the System Controller runs.

All of the Hss Service's instances run traffic simultaneously and if the HssServer module (process) fails on an instance of the Hss service, the whole service fails on that SBC and the Hss service instance becomes disabled. The traffic load processed by the failed Hss instance is redistributed by the Diameter peer onto one or all of the remaining active Hss service instances. In such case, no loss of service is perceived by the subscriber. In case of failure of the current active instance, one of the unsassigned-enabled node becomes the new active one. Please see section *Scalable cluster configuration* for more details on scalability.

IMS-HSS

The Home Subscriber Server (HSS) is the main data storage for all subscriber and service-related data of the IMS subscriber. The HSS contains all the user-related subscription data (user profile, number of features and services associated to it) required to handle multimedia sessions. The HSS supports the Cx/Dx and Sh/Dh interfaces and is compliant with Release 7 of 3GPP. The primary objective of the HSS is to provide subscriber profile information on the IMS network and routing information with the Subscription Locator Function (SLF) functionalities. The subscriber profile information exchanged between the HSS and the CSCF/AS contains the following:

- Subscriber identity
- Subscriber services and profiles
- Service specific information
- Mobility management state

The information exchanged between the SLF and the CSCF/AS contains the following:

- Routing Information (The Name of the HSS that is hosting a particular subscriber within a network where many HSS are deployed.)

To be able to make the exchanges of the information mentioned above, the HSS stores the following user related information:

- User Secret key or Operator Secret key that is used to compile the Authentication vector;
- User Numbering and Addressing information;
- User Location information at inter-system level: the HSS supports the user registration, and stores inter-system location information;
- User Security information: Network access control information for authentication and authorization;

- User Profile information related to the service logic and service location.

To be able to make the exchanges of the information mentioned above, the SLF functionality in the HSS stores the following information:

- Subscription Locator Function information (HSS Names and Public Identities) for routing purposes in the case where multi-HSS are deployed.
- List of Public Identity with their corresponding HSS Name in which they are hosted.

The HSS contains the actual logic required to satisfy both the 3GPP Diameter Base Protocol specifications and the Cx/Dx and Sh/Dh applications requirements for all Cx/Dx messages:UAR, SAR, LIR and MAR, RTR and PPR messages, as well as all Sh/Dh messages: UDR, PUR, SNR and PNR

Hence, the HSS Server of the HSS cannot only send responses to messages invoked by the CSCFs or the AS, but can also inform them of changes made to user profiles and/or charging information by notifying the CSCFs appropriately with the Cx-Deregister and Cx-Update_Subscr_Data messages: RTR and PPR and can also notify the AS of any changes made in subscriber profiles related to service with the Sh-Notif and Sh-Notif-Resp messages: PNR and PNA.

The HSS communicates with IMS Network entities such as CSCFs and Application Servers. For entities located in the same home network as the HSS, the HSS communicates with the CSCFs through the Diameter Cx interface and with the Application Servers, through the Diameter Sh interface. In the case where multi-HSS are deployed, with the Subscription Locator Function functionalities of the HSS, it can also communicate with the CSCFs and AS through the Dx and Dh interfaces.

In the case where multi-HSS are deployed, the Subscription Locator Function functionalities of the HSS, allow a CSCF/AS to easily find in which HSS a particular subscriber is hosted. The CSCF/AS only need to use the Dx/Dh Diameter interface to get the benefits of that functionality.

The HSS application interfaces with the database in order to retrieve profile information, permanent subscriber data entered by the operator during subscriber provisioning, location information and temporary subscriber data. The SLF functionality of the HSS interfaces with the database in order to retrieve routing information.

The HSS provides service provisioning support to the AS by exchanging data related to application and service triggers (Subscribed Media Profile Identifier, Initial Filter Criteria, Application Server Information and Service Indication) through the Diameter Sh interface.

The HSS supports:

- TCP transport protocol
- IPSec security transport

The system that the HSS runs on consists of a number of Single Board Computers (SBCs).

Each blade is assigned specific subsystem function during the system provisioning process. The following subsystem functions are required to configure HSS:

- System Controller
- IP Gateway - provides primary IP interface to the system. Provides termination point for TCP based connections and uses distribution function to route the Diameter traffic to the active HSS servers.
- HSS Server - provides processing of the Diameter AVPs for the Cx/Dx, Sh/Dh interfaces.

The HSS functional entity is a database in charge of the management of mobile subscribers in the IMS network.

A PLMN (Public Land Mobile Network) may contain one or several HSS: depending on the number of mobile subscribers, on the capacity of the equipment, and on the organization of the network.

In the case where a PLMN contains several HSS, the SFL functionality of the HSS can be enabled to take care of redirecting the Diameter queries from the CSCF or SIP Application Servers to the right Home Subscriber Server. The SLF functionality helps the CSCF/AS to find in which HSS a particular subscriber is hosted. The CSCF and SIP AS will send Diameter queries (UAR, SAR, MAR, etc.) to the SLF when they do not know which HSS holds the subscriber record. The SLF functionality being implemented in the HSS Server process, the CSCF and SIP AS will send Diameter queries to the enabled SLF functionality of the HSS. The CSCF will use the Dx interface (similar to Cx) and the Sip-AS would use the Dh interface (similar to Sh) to exchange information with the SLF. To these Diameter queries, the SLF functionality of the HSS is in charge of finding the name of the HSS hosting the subscriber in the HSS's database. Moreover, the SLF will answer to each Diameter Message with an answer that includes an additional Diameter-Redirect-Host AVP that contains the name of the HSS that hosts the subscriber. The ResultCode of each Dx/Sh answer sent by the SLF is `DIAMETER_REDIRECT_INDICATION` if the public Identity has been configured in the SLF with its HSS Host name.

AAA

The AAA Server provides RADIUS-based Authentication, Authorization and Accounting functionalities and contains all subscriber information for subscribers of the RADIUS AAA functionality. Moreover, the AAA Server provides WiMAX functionalities. For a description of the WiMAX functionalities supported by the AAA Server, refer to section *AAA*.

The AAA Server is integrated with the HSS Server process and operates as part of the Hss Service on a single Board Computer.

When the AAA Server functionality is enabled in the SDM configuration one or more virtual IP addresses are assigned to the AAA Server via the configuration. The AAA Server will process RADIUS IP traffic on these addresses.

Since it is part of the HSS Service, the AAA Server also runs in an active/unassigned (1+N) mode. When multiple AAA virtual IP addresses are defined, the task of processing traffic on these interfaces is distributed across all AAA Server SBCs, i.e. all instances of the Hss Service. Furthermore, when one SBC fails, the AAA virtual IP addresses are automatically relocated to another active SBC running the Hss Service. Since the AAA IP connections are based on UDP, this relocation is invisible to the RADIUS client nodes on the network.

ENUM

The ENUM Server provides DNS-based telephone number mapping functionalities. For a description of the ENUM Server's behavior and functionalities, refer to section *ENUM* of this document.

Just like the AAA Server and the SLF, the ENUM Server is integrated with the HSS Server process and operates as part of the Hss Service on a single Board Computer. Refer to the beginning of *HSS Server* for more details on the HSS Server process.

HSS authentication center

The HSS Authentication Center provides authentication to users on the IMS network. The Authentication Schemas supported are the

- Digest (defined by the Packet Cables)
- Digest AKA V1-MD5
- Digest-MD5
- HTTP_DIGEST_MD5

- NASS-Bundled

The ETSI TISPAN defines the algorithms for the HTTP_DIGEST_MD5 and NASS-Bundled Schemas. In the HSS AuC, specific algorithms can be provisioned for the supported Schemas. The HSS AuC interfaces with the telecommunication network through the corresponding Diameter messages as defined in the applicable Diameter specifications.

As the Akav1 MD5 is based on GSM Milenage algorithm, the HSS provides a way to define specific Gsm Milenage algorithm by setting the variant part of the algorithm like OP, Amf, C1-C5, R1-R5 values. These values are used in the algorithm to generate the Quintuplet vector. These values are variants in the algorithm and are set to the default values. HSS AuC allows you to specialize and define your own algorithm to ensure you a more robust encryption.

The HSS Authentication Center is integrated with the HSS Server process and operates on the Hss Service on a Single Board Computer.

The Hss Service runs in an active/unassigned (1+N) redundancy mode. This means that there can be multiple instances of the Hss Service, all providing service, one in an active state and all others in an unassigned state. With an HSS AuC being integrated in each Hss Service instance, we can say that the HSS AuC also operates in active/unassigned (1+N) redundancy mode. In the case of failure of a Hss Service instance, the traffic load of that instance will be redistributed throughout all the other active Hss Service instances. Please refer to *Services Running on the System* for more details on the redundancy mode of the Hss service.

HSS Provisioning Manager

The HSS Provisioning Manager is a module running within the DataAccess service (User Service).

If the HssProvManager module (process) fails on an instance of the DataAccess service, the whole service fails on that blade, the DataAccess service instance becomes disabled and the load is redistributed among the remaining active DataAccess service instances on the other blades. In such case, no loss of services is perceived by the subscriber and the capacity of the system remains the same. See *Services Running on the System* for more details on the redundancy mode of the DataAccess service.

The HSS Provisioning Manager process is used to validate subscriber data entered into the database by the operator. One of its main functions is to verify the consistency of new data entered in the database with existing data. Some services are mutually exclusive and others require previously configured information.

The actual field validation like acceptable ranges, type checking, etc. is done by the OAM&P Manager at a generic level based on the global schema.

Inherent validation at the relational database level is also performed for deletion and creation of records.

The HSS Provisioning Manager maintains all IMS HSS related subscriber data: i.e. IMS subscriber profiles and AAA subscriber profiles.

Policy Provisioning Manager

The Policy Provisioning Manager is a module running within the DataAccess service (User Service). This process handles all Policy (SPR) provisioning requests queried to the system.

If the Policy Provisioning Manager module fails on an instance of the DataAccess service, the whole service fails on that blade, the DataAccess service instance becomes disabled and the load is redistributed among the remaining active DataAccess service instances on the other blades. In such case, no loss of

services is perceived by the subscriber and the capacity of the system remains the same. Please see section for more details on the redundancy mode of the DataAccess service.

The Policy Provisioning Manager process is used to validate Policy subscriber data entered into the database by the operator. One of its main functions is to verify the consistency of new data entered in the database with existing data. Some services are mutually exclusive and others require previously configured information.

The actual field validation like acceptable ranges, type checking, etc. is done by the OAM&P Manager at a generic level based on the global schema.

Inherent validation at the relational database level is also performed for deletion and creation of records.

The Policy Provisioning Manager maintains all Policy related subscriber data.

A single instance of the Policy Provisioning Manager runs within the DataAccess service on each of the SBCs, in an active/unassigned (1+N) mode where all enabled instances process requests. In the case of failure of a DataAccess instance, the traffic is redistributed over the remaining enabled instances.

LTE HSS Server

The Tekelec Long Term Evolution-Home Subscriber Server (LTE-HSS) serves as the primary database repository of subscriber information within Evolved Packet Core (EPC) (also known as the System Architecture Evolution (SAE)) networks. The LTE HSS Server exchanges messages with an MME or a SGSN using the Diameter Protocol (defined by the IETF in the RFC3588) over TCP or SCTP.

The main roles of the LTE-HSS Server are as follows:

- To serve as a registration and authentication server for mobile subscribers in the EPC network
- To track the LTE subscribers' mobility by acting as the real-time location repository and updating their position in administrative areas handled by MMEs/SGSNs.
- To send the subscriber data profile to a MME/SGSN when a subscriber first roams there and to remove the subscriber data from the previous MME/SGSN when a subscriber has roamed away from it.

The LTE-HSS is capable of supporting authentication and bidirectional roaming between 3G-LTE networks by either communicating with the HLR Server (SDM ngHLR) or with the HLR Server's HLR-proxy functionality to forward messages to a legacy HLR.

The LTE-HSS Server is 3GPP Release 9 compliant and has been fully integrated with the GSM/UMTS ngHLR, which means that it shares the following with the Tekelec ngHLR:

- subscriber profile
- volatile data
- AuC
- SW/HW platform
- provisioning stream

For a more detailed description of the LTE-HSS's functionalities, refer to the section *LTE-HSS features* of this document.

The Diameter interface used between the LTE-HSS Server and the MME is named S6a while S6d is the one used between the LTE-HSS Server and the SGSN.

Through these interfaces, the LTE-HSS Server supports the following types of messages:

- Update Location Request/Answer (ULR/ULA), Cancel Location Request/Answer (CLR/CLA), Purge UE Request/Answer (PUR/PUA) messages for Location Management procedures
- Delete Subscriber Data Request/Answer (DSR/DSA), Insert Subscriber Data Request/Answer (IDR/IDA) messages for Subscriber Data Handling Procedures.
- Reset Subscriber Request/Answer (RSR/RSA) messages for Fault Recovery Procedures.
- NotifyRequest/Answer (NOR/NOA) messages for Notification Procedures.
- Authentication Information Retrieval/Answer (AIR/AIA) for Authentication Procedures.

The LteHssServer is the process of the LteHss Service which runs on the SBCs (Single Board Computers). Multiple instances of the LteHssServer can run on each SBC in an active/standby/unassigned state, following the 1+N redundancy model (contact Tekelec's Customer Support for a plan of the recommended SDM architecture and configuration as per your needs). This means that there is one active instance and N unassigned instances of the LteHss service that run simultaneously on the system. Moreover, a threshold of one instance can run on the system in order to provide service (minimum number of active service instances needed to continue to provide services). In this model, all the instances provide service granted of course that they all are enabled (OpState). The unassigned instances all refer to the active instance.

In a two and four SBC system, an instance of the LteHss service can run on the SBC on which the System Controller runs; however, in an eight, twelve or sixteen SBC system, an instance of the LteHss service should run on a blade provisioned with the FrontEnd identity and shouldn't run on the SBC on which the System Controller runs.

All of the LteHss Service's instances run traffic simultaneously and if the LteHssServer module (process) fails on an instance of the LteHss service, the whole service fails on that SBC and the LteHss service instance becomes disabled. The traffic load processed by the failed LteHss instance is redistributed by the Diameter peer onto one or all of the remaining active LteHss service instances. In such case, no loss of service is perceived by the subscriber. In case of failure of the current active instance, one of the unassigned-enabled node becomes the new active one . Please see section *Scalable cluster configuration* for more details on scalability.

Equipment Identity Register (EIR)

The EIR stores international mobile equipment numbers (IMEIs), which identify the physical handset when accessing the network. The operator can assign individual IMEIs or IMEI ranges to white (allowed), black (blocked) or gray (track) lists, or to list combinations. While the handset does not identify the subscriber, the operator can associate the handsets IMEI with the subcribers IMSI, which is part of the subscriber identification.

Multiple IMEIs can be associated with one IMSI, for example, when the subscriber has more than one device on the same account. Multiple IMSIs can be associated with one IMEI, for example, when the subscriber uses the same SIM card for multiple devices.

When configuring the EIR, IMEIs can be already bound to a subscription or unbound when used for independent EIR deployment.

The operator can provision and maintain the EIR database completely on the local network, or choose to use an interface between the networks EIR database and the Central EIR (CEIR) database in Dublin, Ireland, which contains daily updated lists of authorized and unauthorized IMEIs from operators around the world.

Tekelec simplifies IMEI screening by integrating advanced database management and signaling functions. When a subscriber roams, the handset attempts registration with the mobile switching center (MSC) and visitor location register (VLR). A standard mobile application part (MAP) message

queries the EIR database about the status of the handset, and the EIR returns a response based on the database information available. The EIR also has a global response option which allows a default response to be returned, regardless of the actual status of the IMEI, or even the presence of the IMEI, in the database.

For the EIR to determine a response or an action, an EIR search proceeds as follows:

- Searches for a matching unbound IMEI and uses the resulting equipment status if found. Then,
  - checks if IMEI/IMSI exists in unbound association table and overrides black list condition if needed
  - if dynamic IMSI recording is enabled and the IMEI/IMSI is not in the unbound association table, it will be added
- If no matching unbound IMEI is found, searches for a matching bound IMEI and uses the resulting equipment status if found. Then,
  - checks if IMEI/IMSI exists in bound association table and overrides black list condition if needed
  - if dynamic IMSI recording is enabled, and the IMEI/IMSI is not in a bound association table, it will be created
- If no matching unbound or bound IMEI was found, searches the IMEI Range table for ranges that include the given IMEI, and uses the OR condition of all resulting equipment statuses if found

Configuration

EIR can be configured through SOAP/XML, XML, LDAP, Bulk Load using XML, UI To set up EIR, the operator configures the equipment status (IMEIs and their associated lists), global message responses, which apply to all EIR features, and other response types based on equipment status and subscriber associations.

Using WebCI, configure

- Common EIR settings that apply to all EIR applications on the same node in **EIR ➤ EIR Configuration**. The common EIR settings include the EIR response types.
- Associations for bound IMEIs and dynamic IMSI recording in **Subscription Management ➤ Subscriber Provisioning ➤ EIR ➤ display/modify**.

Performance

Performance counters measure the following items:

- Number of ECR messages received
- Number of ECA messages sent when the Global Response is either active or inactive for each list type (white, grey, black, unknown)
- Number of black listed IMEIs overridden due to association with a matching IMSI
- Number of black listed IMEIs with a non-matching IMSI
- Number of dynamically associated IMSIs
- Number of white/grey/black-listed IMEIs defined in the system
- Number of white/grey/black-listed IMEI ranges defined in the system

Logs

Every EIR that results in the sending of a gray- or black-listed response, or a white-listed response for a black-listed IMEI, results in a log message, which is stored in the EIRLog file.

The Audit Manager generates and maintains log files. Log files are enabled or disabled through the CLI and WebCI (Oamp>AuditManager). Log files use either the CSV or XML format and can be configured for the number of days that old log files are kept. The log files are stored in the directory /export/audit, on both active and standby System Controller servers. The file EirLog.xml has the most recently generated logs.

LTE Equipment Identity Register

The long-term evolution (LTE)-EIR feature integrates EIR into the LTE network by using the diameter protocol with S13 interfaces:

- The S13 interface is defined between the EIR and the MME (Mobility Management Entity).
- The S13 interface is defined between the EIR and an S4-SGSN.

Both interfaces run on top of the TCP or SCTP protocol, which transfers signaling messages.

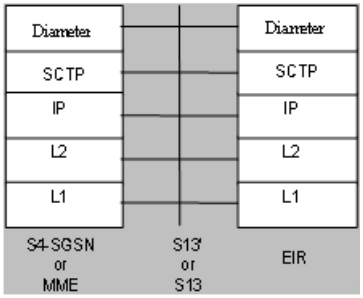


Figure 14: Diameter stack

LTE-EIR supports the Diameter ME-Identity-Check-Request (ECR) command. Upon receipt of such a message and based on database information, the LTE-EIR computes an ME-Identity-Check-Answer (ECA). mobile stations or For example, (1) when the MS roams into a new serving eUTRAN area, it transmits an Attach Request to eNodeB. (2) After determining that a new MME is requested, eNodeB forwards the Attach Request to the new MME. (3) Before continuing with the Attach procedure, the MME sends an ME Identity Check Request (ECR) to the EIR to confirm the IMEI or IMEI-IMSI combination. (4) The EIR then retrieves the IMEI or IMEI-IMSI combination from the message and searches the EIR database for a match. The search may result in IMEIs being on the white, grey, or black list or in an invalid IMEI-IMSI combination. Based on the result, the EIR returns an ME Identity Check Answer (ECA), which contains either the equipment status (allowed/not allowed) or a Result Code with error

Configuration

LTE-EIR is part of the LTE-HSS user service but can be enabled separately from LTE-HSS. If they are enabled together, they require different fully-qualified domain names (FQDNs) and different TCP/SCTP ports. LTE-EIR can be enabled on multiple blades for fault tolerance.

LTE-EIR configuration requires Diameter provisioning for LTE-EIR and the provisioning of the LTE-EIR to provide the correct responses for equipment status and both bound and unbound IMEIs:

Using WebCI:

- The LteHss user service is enabled in **System ➤ Service Management**.
- Diameter is configured in **LTE-EIR ➤ LTEEIR configuration**.
- Common EIR settings that apply to all EIR applications on the same node are configured in **EIR ➤ EIR Configuration**. The common EIR settings include the EIR response types.

Associations for bound IMEs are created in **Subscription Management ➤ Subscriber Provisioning ➤ EIR ➤ display/modify** and includes dynamic IMSI recording.

Ras Server

The Ras Server's role is to support queries from the XML-REST interface. It is responsible for:

- Receiving and validating XML-REST queries
- Converting the XML-REST queries into XML requests
- Forwarding the XML requests to the Data Access Server, which handles and manages the policy data through the Policy Provisioning Manager module and as a result stores it into the database.

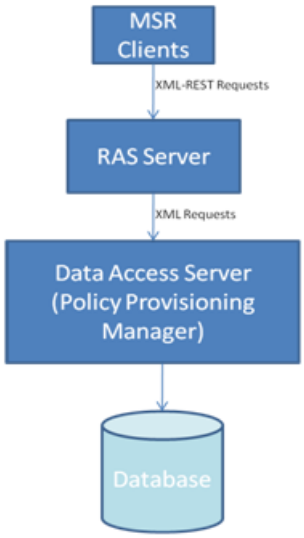


Figure 15: RAS Server

The RasServer is the process of the Ras service which runs on each of the SBCs (Single Board Computers). One instance of the RasServer can run on each of the SBC blades in an active/unassigned state, following the 1+N redundancy model (contact Tekelec's Customer Support for a plan of the recommended SDM architecture and configuration as per your needs). This means that there is one active instance and N unassigned instances of the Ras service that run simultaneously on the system. Moreover, a threshold of one instance can run on the system in order to provide service (minimum number of active service instances needed to continue to provide services). In this model, all the instances provide service granted of course that they all are enabled (OpState). The unassigned instances all refer to the active instance.

All of the Ras Service's instances run traffic simultaneously and if the RasServer module (process) fails on an instance of the Ras service, the whole service fails on that blade and the Ras service instance becomes disabled. The unassigned instances all refer to the active one and in case of failure of an instance, the instances that remain enabled take on the load of the failed instance in addition to their

already assigned load. In case of failure of the current active instance, one of the unsassigned-enabled node becomes the new active one. Please see section *Ras Server* for more details on scalability.

The Ras server is configured at installation by Tekelec's *Customer Care Center*. For information on the Ras Server's configuration parameters, refer to the "Service Option" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. For instructions on how to view/troubleshoot the RAS server configuration data from the WebCI, refer to the "Configuring the RAS Server (XML-REST interface)" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide.*

System Controller

The main function of the CoreSystemController (CoreSC) Service is to act as the reference database for configuration and provisioning of subscriber profiles and to provide a single and unified interface for Operation, Administration, Management and Provisioning (OAM&P). All information from other subsystems is aggregated at the CoreSystemController Service and presented to the operator through a command line interface (CLI) or graphical user interface (WebCI). Also, the CoreSystemController Service manages the allocation of software functions to individual blades, maintains the in-chassis topology, and maintains policies and status for the health of the system.

Only two System Controller Identities can exist in a shelf and their associated CoreSystemController Service always runs in an active-standby mode. This means that a single instance of the CoreSystemController Service runs on two blades, one instance is in an active state and the other in a hot standby state. This means that vital information of the CoreSystemController Service is constantly replicated to the hot standby instance and in case of failure of the active side of the CoreSystemController Service, the standby side is ready to take over. Please refer to *Services Running on the System* for more details on the redundancy mode of the CoreSystemController service.

Database

The SDM network supports a high-availability database running within the Database service in an active/standby (1+1) mode. This relational database supports transaction with ACID (Atomicity, Consistency, Isolation, and Durability) properties to ensure transactions are processed reliably. It operates in clustering mode through the SDM High-Availability framework. The following figure illustrates the operation context.

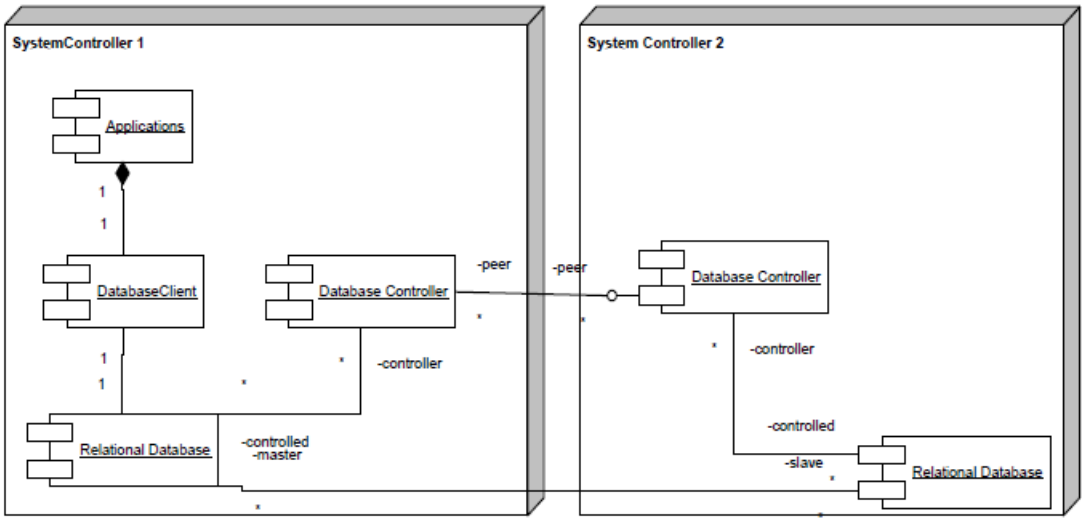


Figure 16: Database component diagram

The database is managed by the DpController and DpProxy modules, which run within the Database service.

Database clients are linked with the database client module, which provides an object oriented interface to the Global Schema. The applications formulate their requests and the database client ensures that the requests are applied against the master database.

The system supports a Database service instance on each System Controller (SC) node, with one reference (active/master) database instance and one replica (standby) database instance.

- The reference database runs in an active/standby (1+1) mode and provides writing/reading services of the database.
- The replica instance is in hot standby mode and can take on the reference role upon failure of the active database instance.

Additional services must be bound to the FrontEnd identity to allow applications remote access to the database of the active and standby SC nodes.

Global Schema

The SDM software is designed using a multi-tiered architecture. Specifically, it provides the following layers of implementation: Application, Session management layer, Global Schema, and Database. The database stores the Tekelec ngHLR and/or HSS information of each layer, from the bottom up.

In its current implementation, there is one highly available relational database per cluster. On top of this, the architecture provides a Global Schema. The Global Schema is a thin layer of abstraction that decouples the physical implementation from the application. It presents an Object Oriented view of the data to applications in the form of Entities, Attributes, and Operations.

The purpose of the Global Schema is to accommodate for scalability and evolution changes in the physical schema without impacting the applications themselves.

Applications formulate Object Query Language (OQL) against the Global schema without having to know the technologies they are interacting with or where they are located. The proxy client tier provides the infrastructure to formulate and dispatch requests for processing.

Applications not running in the context of the SDM system can interact with the system using XML requests via the Session layer. The XML requests are supported by the OAM&P Manager process.

Finally, the architecture provides a presentation layer through the Command Line Loader.

System Management

Both the Command Line Interface (CLI) and Web Craft Interface (WebCI) consoles are supported on the System Controller (SC).

Both the WebCI and the CLI can be used to provision and manage the Subscriber and Service Databases, but the CLI can additionally be used to perform basic debugging in case of Network interface problems. The WebCI provides a more user-friendly approach and the ability to easily view system based alarms and configuration parameters.

The WebCI interface is based on the Secure HTTPS protocol and the CLI includes a User Security Management feature.

Command Line Interface

The Command Line Interface provides the functionality, mainly to CLI.

The Command Line Interface (CLI) is the client OAM&P (Operation, Alarm, Maintenance and Provisioning) application that manages and provisions the SDM. The CLI provides a command-line, text-based environment to access the OAM&P. The operator accesses OAM&P functionality by invoking commands in the CLI. Changes made to system configuration or subscriber provisioning data takes effect immediately. With the User Security Management feature, not all CLI commands and functionalities are available to all users. The administrator of the system is in charge to create and manage users, their username and password and assign them to groups with different access privileges for specific services.

Only the administrator is allowed to perform all the tasks in CLI, as follows:

- Create and manage users.
- Manage Dynamic System Configuration.
- View, add, delete, and modify subscriber provisioning information.
- View and modify configuration data.
- View and modify operational aspects of the system
- View and modify system configuration properties
- View current and historical data
- emote system administration
- System maintenance

Refer to *Security management* for a more detailed description of the User Security Management feature, also refer to the *User Management* section of the *SDM System Configuration - Reference Manual*, and to *Creating and Managing users for the User Interfaces* in the *SDM System Configuration - User Guide* for step-by-step procedures to provision users through CLI and WebCI.

Auto completion

The Command Line Interface (CLI) supports the auto completion functionality. When starting to enter a command, the command can be automatically completed by pressing the **<tab>** key. When more than one option is available, all the options will be displayed when the **<tab>** key is pressed.

WebCI

The Web Craft Interface (WebCI) is an integrated web-based application that provides a user friendly graphical user interface (GUI). The GUI is used to facilitate system configuration, subscriber provisioning, and alarm management.

Web browser

The Web Craft Interface (WebCI) supports the following versions of web browsers:

- Internet Explorer version 8 on Windows.
- Mozilla Firefox version 12.0.

WebCI navigation

The WebCI main menu is located to the left of the window. The menu provides access to the SDM applications.

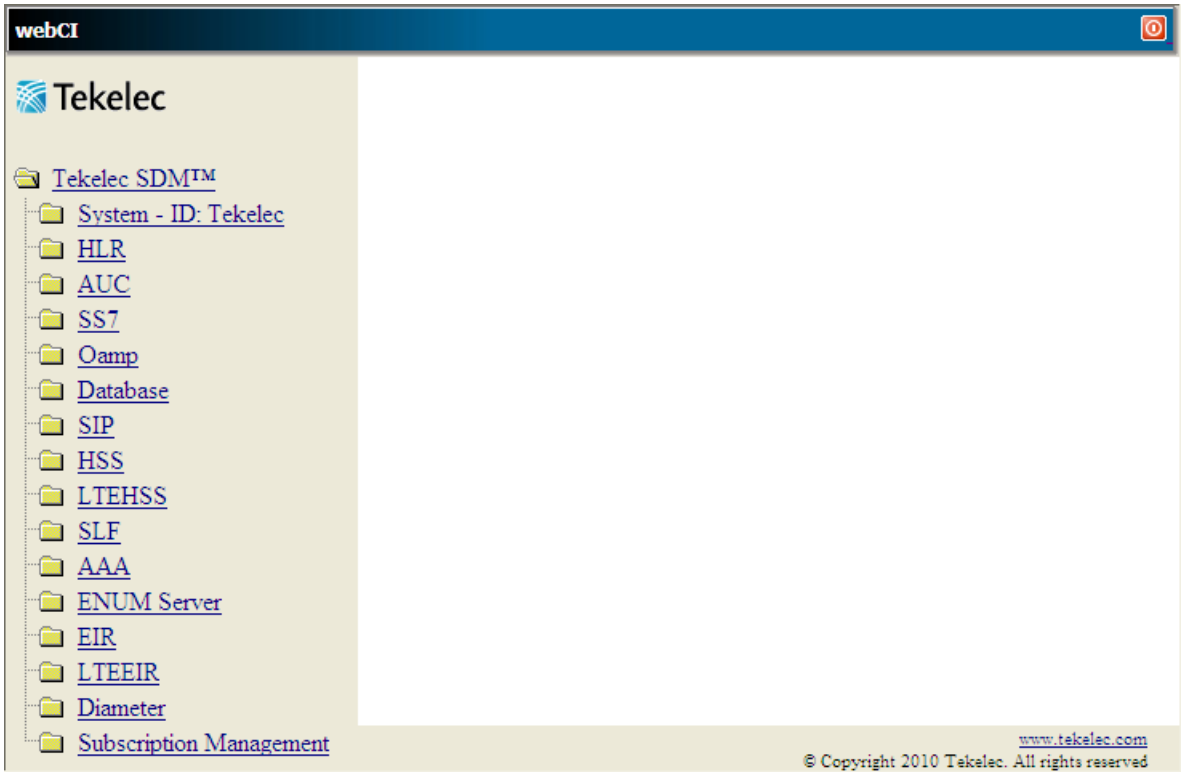


Figure 17: WebCI main window

Clicking the application name or folder opens a submenu. Each submenu item has a specific configuration window.

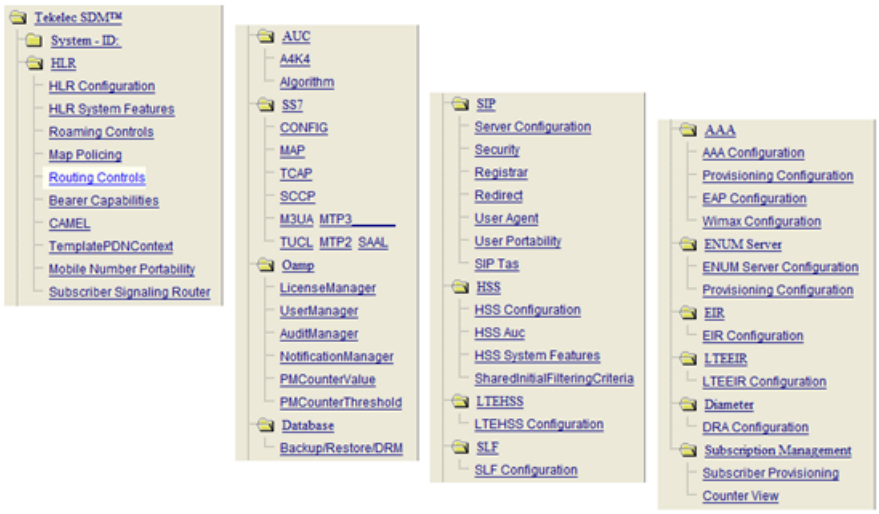


Figure 18: WebCI main menu expanded

These windows may have tabs to access additional configuration settings.

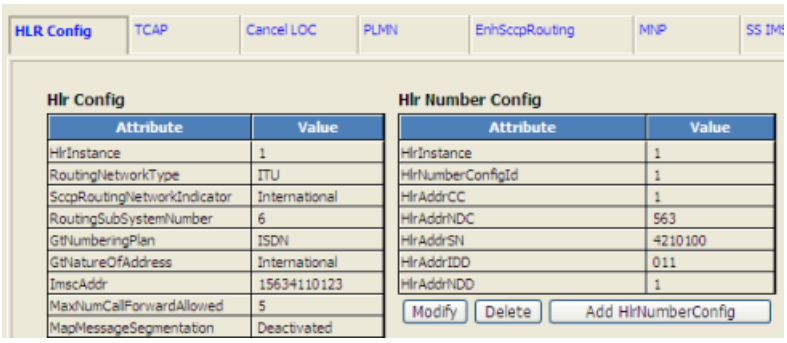


Figure 19: WebCI window tabs

WebCI main menu descriptions

This table describes the purpose of each menu item. The items are listed in order they appear on the menu.

Table 5: WebCI main menu descriptions

Application	Folder	Description
System	**Shelf View**	Provides information on each of the hardware platform's slots (processors) and the services running on each one of them. This window allows to configure the system with identities/services on each slot. This view also allows to perform Switch Overs.
	Shelf Inventory	Displays Shelf information and the software version.
	Service Management	Provisions services to each slot's Identity. Also allows the operator to manage those services on each slot.

	Geo Redundancy View	Provides information on the geo-redundant feature, whether it is enabled or disabled and what the Geo-Redundancy Virtual IP (VIP) address of the peer site is, as well as information on the state of the database. It also allows to enable or disable the feature and to modify the Geo-Redundancy VIP address of the peer site.
	Active Alarm View	Provides a listing of all active alarms existing on the shelf.
	History Alarm View	Provides a listing of all alarms that have occurred as well as those that have been cleared on the system.
HLR	**HLR Configuration**	This window is divided into the following tabs: HLR Config: allows to provision HLR Configuration parameters, HLR Number Configuration, and HLR SIP Subscriber Information for MAP SRI Interworking with SIP Subscribers. • TCAP: allows manual execution of the TCAP out-of-service and TCAP in-service operations. • Cancel LOC: allows manual execution of a Cancel Location and a Cancel GPRS Location. • PLMN: allows manual provisioning of Plmns and Home Plmns. • MNP: allows manual activation/deactivation of the Mobile Number Portability functionality. • VlrMsgNotification: allows manual activation/deactivation of the XML Notifications on UL, GPRS-UL, SAI, Ready SM, Purge MS and CL.
	HLR System Features	Provisions USSD messaging handling parameters such as Service Code, Application Node, and Application Node address. Moreover, it allows to configure the following HLR features: FTN Management, FTN Digits Analysis, XML notification on NDC change, Short Number Translation on RegSS.
	Roaming Controls	Provisions PLMN and IMSI Rejection error causes, VLR/PLMN Definitions, OCPLMN templates, Allowed IMSI ranges and Service Screening Templates.
	MAP Policing	Defines custom templates by provisioning Application Context templates and AcTemplateMapping to associate each of these templates to a node number. It also displays the NodeNumber and NodeNumberAcMapping tables. It also enables the operator to force the Tekelec ngHLR to send MAP_Reset messages to peer nodes.
	Routing Controls	Allows the Network Operator to: • Define Destination Router addresses

		• Define Routing Templates for the GSM/IMS Router (MT-SMS/SRI/SRI-LCS/ATI routing). Defining a routing template consist mainly in setting the following:
		  • Routing trigger
		  • Routing type
		  • Destination Router
		  • Default Action
		• Define Routing exceptions (only applies for MT-SMS routing)
		• Define a subscriber IMSI for Redirect Routing (only applies to MT-SMS routing)

	Bearer Capabilities	Provisions different types of Bearer Capability information, each identified by a unique BearerCapName to which MSISDNs can be associated to when provisioning the subscriber profile.
	CAMEL	Provisions the HLR Camel USSD General Csi parameters, Camel GSM Service Control Functionality and the CamelServiceMaskTemplate for enhanced CAMEL handling.
	TemplatePDN Context	This window allows to define PDN Context Templates for the LTE-HSS profiles. Each PDN Context provisioned for a LTE-HSS profile must have a PDN Context Template assigned to it.
	Mobile Number Portability	Provisions the Mnp entity in order to provision the Number Portability data for each "ported" MSISDN and the ImsiForRedirect entity in order to provision the IMSI that must be returned in the SRI-ack when the Tekelec ngHLR redirects the interrogating node to the recipient's network.
	Subscriber Signaling Router	Activates/Deactivates SSR (Subscriber Signaling Router functionality) and provisions SSR Templates and assigns them to an IMSI or IMSI range and to a MSISDN or MSISDN range.
AUC	**A4/K4**	Provisions the A4/K4 Transport Encryption Algorithm by defining A4/K4 combinations.
	Algorithm	Provisions the Authentication algorithms that will be used to authenticate subscribers.
SS7	**CONFIG**	Allows to view the activation status of the SS7 and SIGTRAN links
	MAP	Provisions MAP general parameters, SAP, Application context, and Timer profile.

	TCAP	Provisions TCAP general parameters, SAP, and Timer profile.
	SCCP	Provisions SCCP general parameters, Timer profile, Network SAP, User SAPs, Route, Concerned Area, Global title entries and SCCP addresses.
	M3UA	This is part of the SIGTRAN protocol. It is used to provision M3UA general parameters, Network, Network SAP, SCT SAP, PSP, PS and Route.
	MTP3	Provisions MTP3 general parameters, Network SAP, Timer profile, Signalling points, Combined Linksets, Linksets, Links, and Routes.
	MTP2	Provisions MTP2 general parameters, Service Access Point (SAP), and Timer profiles.
	SAAL	Provisions SAAL general parameters and Service Access Point (SAP).
	TUCL	This is part of the SIGTRAN protocol. It is used to provision the TUCL general parameters and the TUCL Sap (TSap).
Oamp	**License Manager**	Displays the License information and allows to view the number of active subscribers at the end of each month. It also allows to provision active and total thresholds.
	User Management	Manage users, following the USM feature, the group they are in and their password as well as their access privileges.
	AuditManager	Provisions: The AuditManager entity: • The Audit log message format (CSV or XML) • The number of days that the old audit log files must be kept in the /export/audit director. • The debug information request in order to request the following debug information to be included in each audit line: slot, module, file and line. By default, this debug information is not included. The AuditInfo entity: • The new AuditInfo entity has been implemented to allow the Network Operator to view the information that is being audited and its audit status: Enable or Disable.
	NotificationManager	Manage notification subscription permissions/properties for each application and users.
	PMCounterValue	Allows to view the current value of OS Resource and HLR Subscriber counters.

	PMCounter Threshold	Allows to view and edit the thresholds implemented for the OS Resource counters.
Database	**Backup/Restore/ DRM**	Performs a manual backup and a restore of the entire database file or individually of some portions of the database. Can also perform an automatic backup of the subscriber's profile data. Also allows to manage the self healing functionality of the system (Database Monitoring Replication).
SIP	**Server Configuration**	Provides information on the SIP Configuration attributes and their values as well as on the Sip IP Configuration.
	Security	Provides information on the SIP Security Configuration attributes and their values.
	Registrar	Provides information on the Registrar Configuration and its Domain and provisions the RegistrationBinding.
	Redirect	Provides information on the SIP Redirect Configuration's attributes and their value.
	User Agent	Provides information on the SIP User Agent Configuration, the SIP User Agent Register Configuration, the User Agent PersistentContact and the IP User Agent Configuration attributes and their values. It also provides information on the UaRegistrationBinding.
	User Portability	Provides access to the NpAorUseRangePrefix table, which defines Address of Record user range prefixes.
	SIP Tas	Allows the Network Operator to conigure Telephony Application Server (TAS) data (Gt, Tt, Prefix, TasId, TasFQDN, OverrideTt, etc.). The SDM extracts the TAS data configured here when redirecting/relaying messages to an external TAS.
HSS	**HSS Configuration**	Provides information on the HSS Configuration, HSS Configuration TCP Listen Address and HSS Configuration SCTP Listen Address, their attributes and their values. Also allows the provisioning of HSS parameters such as HSS Configuration Destination Realm and HSS Configuration Destination Hosts.
	HSS AuC	Allows to configure the Authentication schemas and algorithms that will be used to authenticate IMS subscribers.
	HSS System Features	Provisions HSS Subscriber configuration parameters, such as HSS Charging Info, HSS S-CSCF Server, HSS Authorized Visited Network and HSS AS Permanent list. It also allows to configure the SPR by defining the Service Indications supported by the SPR from the Sh interface and from the OAM&P provisioning interface, setting the

		Auto Enrollment feature and data compression level, and configure internal receive queue, sequential write/read/write requests, as well as HTTP and XML-REST request processing.
	SharedInitial FilterCriteria	Provision the Shared Initial Filter Criteria feature by allowing to define Shared Initial Filter Criterias and for each of them a list of Shared Service Point Triggers.
LTE-HSS	**LTEHSS Configuration**	Provides information on the LTE-HSS Configuration, LTE-HSS Configuration TCP Listen Address and LTE-HSS Configuration SCTP Listen Address, their attributes and their values. Also allows the provisioning of LTE-HSS parameters such as LTE-HSS Configuration Destination Realm and LTE-HSS Configuration Destination Hosts. Finally this window offers access to another window through the PLMN tab. This window allows to define allowed PLMNs for specific IMSI Ranges. This is used to allow/disallow roaming to subscribers depending on their IMSI Range and the PLMNs defined in this window.
SLF	**SLF Configuration**	Provides information on the SLF Configuration, SLF Configuration TCP Listen Address and SLF Configuration SCTP Listen Address, their attributes and their values. Also allows the provisioning of SLF parameters such as SLF Configuration Destination Realm and SLF Configuration Destination Hosts.
AAA	**AAA Configuration**	Provides information on the AAA Configuration, AAA System Accounting Servers, AAA Network Access Servers and AAA NAS Accounting Servers, their attributes and their values.
	Provisioning Configuration	Provisions the Dynamic IP Address Allocation functionality by allowing to add, display, modify and delete AAA Address Allocation Policies, AAA Address Allocation Ranges and AAA Address Allocation Associations.
	EAP Configuration	Allows to view and edit the general configuration parameters for the EAP authentication, as well as the configuration parameters for the EAP-SIM, EAP-PSK, EAP-TLS and EAP-TTLS methods. It also allows to provision Server and Root Certificates for EAP-TLS authentication.
	WiMAX Configuration	The Wimax Configuration window provisions: • WIMAX Capabilities • WIMAX Home Agent • WIMAX Qos Descriptor • WIMAX DHCP

ENUM Server	**ENUM Server Configuration**	Allows to provision the following DNS data: • DNS Domain Name List • DNS ENUM User Template • DNS Black List Range • DNS Black List ENUM
	Provisioning Configuration	Allows to view and edit the ENUM Server and DNS Listen Addresses configuration data
EIR	**EIR Configuration**	The EIR configuration window defines: • The common EIR configuration • The IMEI range and associated equipment status for the range • The Diameter host authorized to establish new Diameter connection with EIR application. • Which equipment status to return in ECA if an EMEI has been configured in several lists (White/Grey/Black)
LTEEIR	**LTEEIR Configuration**	The LTE-EIR configuration window configures the Diameter protocol: • Defines Diameter host name and Diameter realm of the EIR for LTE. • Configures IP address for SCTP/TCP connections. • Defines Diameter host authorized to establish new Diameter connection with EIR application. • Defines list of authorized diameter realms
Diameter	**DRA Configuration**	The DRA configuration window configures the Diameter Relay Agent by defining the diameter host name of DRA to connect to the HSS

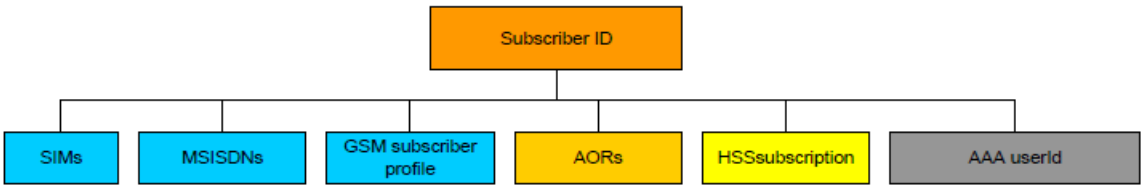
Subscription Management	**Subscriber Provisioning**	The Subscriber Provisioning window:
		• Defines SubscriptionIDs to represent subscribers.
		• Provisions SIM cards assigned or unassigned to a Subscription ID using one of the following operations:
		  • Assign SIM
		  • Unassign SIM
		  • Swap SIM
		  • Display Deferred Swap
		  • Delete HLR Subscriber using the Delete HLRSubscriber button
		  • Search subscriber profiles
		• View/Modify/Add/Delete Policy subscriber profiles

		• View policy quota and state data using the Policy PublicIdentity search • Delete quota data using the Reset Quota button in the Policy PublicIdentity search • View/Modify/Add/Delete an SPR Pool For each subscriber (SubscriptionID), provisions: • IMSIs for the SIM card assigned to the subscriber (SubscriptionID). • MSISDNs for the SIM card assigned to the subscriber (SubscriptionID). • IMSI-MSISDN associations (Primary and alternate) > Multiple IMSIs • HLR Subscriber Profile with a Service Profile in which services such as Call Forward, Call Barring, Closed User Group, Camel Service, Number ID, Call Completion, Call Waiting, and Change Service can be provisioned. Within the Service profile of an HLR Subscriber Profile, an LTE-HSS subscriber profile can also be provisioned. • SIP Subscribers and their AddressOfRecords • HSS Subscribers and their service profile by allowing to create Private Identities as well as Service Profiles and Public Identities. It also permits to create IMS-HSS Initial Filtering Criteria and link Public Identities for different service Profiles. • AAA users by creating AAA User IDs and specifying their Vendor Specific Attributes. • ENUM users • Link Public Identities to HSS Names for SLF Redirect Host Mapping.

SDM Converged Subscriber Management

The SDM system manages all the subscribers and their multi-profiles under one single node.

The SDM manages multi-profile subscribers, which means that it supports and manages subscribers with multiple profiles (HLR, SIP, IMS-HSS/SLF, AAA, WiMAX, DNS ENUM, LTE-HSS) as one unique subscription. Each subscriber is identified by a unique SubscriptionID, which can have one HLR profile and multiple SIP AoRs, IMS-HSS private/public identities, SLF, AAA, LTE-HSS, WiMAX and DNS ENUM definitions assigned to it.



Prior to being able to provision any profile for a new subscriber, the SubscriptionID must always be defined first and it is only once all the profiles have been deleted that a SubscriptionID can be deleted. Each profile can be linked together through the SubscriptionID. For profiles to be linked together, they must refer to the same SubscriptionID.

Refer to the "Subscriptions for SDM subscribers" chapter of the SDM Subscriber Provisioning - Reference Manual for more information on the Subscriptions entity that allows the Network Operator to define SubscriptionIDs.

Refer to the "XML File example for the provisioning of Subscriptions" section of the SDM Subscriber Provisioning - User Guide for instructions on how to provision SubscriptionIDs in bulk using XML files.

SDM Features

Automatic backup

The Automatic Backup creates a consistent snapshot of the subscriber's profile data while the system is active. It will backup all the subscriber's profile data onto the active System Controller (SC). As an additional option, the Network Operator can choose to set the automatic backup to include in the backup, all the configuration data. In this case, the automatic backup creates a snapshot of all the configuration data in addition to one of all the subscriber profiles data.

An automatic backup can be set and activated through the CLI and the WebCI. To have more details on the step-by-step procedures to set, activate, modify or deactivate an automatic backup, please refer to the "Creating a Backup of the system" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Automatic backups are executed and stored on the active blade. The automatic database backup can be set up to launch following these configurable parameters:

- Hour
- Minute
- BackupDirectory
- FileRotation
- IncludeConfiguration

For more details on the configurable parameters used to set an automatic backup, please refer to the "Database Operation" chapter of the *SDM Monitoring, Maintaining, Troubleshooting - UserGuide*.

Partitioned Backup

A manual backup of the database can be performed by the operator through the CLI and the WebCI. To do so, you need to specify the BackupDirectory and use the Backup operation. For more details

and the step-by-step procedures on performing a manual backup, please refer to the "Creating a Backup of the system" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

The operator can perform a manual backup to create a full consistent snapshot of the database while the system is active. It will backup all the subscriber's profile data, system configuration, and alarm history onto the active System Controller (SC). However, the Partitioned Backup feature introduces the possibility of not only performing a manual backup of the entire database, but also having the choice to only perform a manual backup of segments of the database. The operator can choose to only manually backup either:

- The subscriber's profile data
- Alarms
- OamConfiguration
- HlrConfiguration
- HssConfiguration

User Security Management (USM)

The User Security Management feature's role is to:

- Secure the system access from unauthorized users and to grant access to provisioning and maintenance of the system only to qualified operators. The USM enables a system administrator to create different users/groups/services with different privileges or different access rights to the entities of the system. To simplify the management of the different users and entities, there are user groups and entity services that are predefined. An entity service is a grouping of entities of the same functionality. User groups have access permissions for the different entity services. The level of granularity to associate access permission is the entity's service, to simplify the management of the access permission.
- Verify and control the notifications to external applications. The USM enables the Network Operator to control which user is allowed to request which type of notification.The OAMP Notification Manager 'Application Identity', 'UserAppMap', 'NotifSubscribe' and 'ApplProperty' entities have been implemented in order to allow the system's administrator to define the properties and notification registration abilities of each application and the logging options of each application for specific users. At installation, there is a set of pre-defined applications which are in fact, the SDM interface applications: CLI, WebCI, SOAP, CmdFileLoader and LdapDataServer. When a new application wishes to connect to SDM system, the Network Operator must add that application's name in the list, so that the connection can be granted.The application must provide its identity during connection for authentication purpose. The notification subscription can still be done by the application at run-time.

For a detailed description of each of these entities, refer to the "Notification Security Management" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. For instructions on how to provision these entities, refer to the "Creating and Managing users/applications for the Notifications" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

For more details on the user security and on the external connections and requests logging, please refer to *User Security* and *External connections and requests logging* in this document.

Dynamic Configuration

With the Dynamic Configuration feature, the administrator of the system now has the capability of configuring the software and hardware component of the system. This includes, the capability to

manage system expansion using automatic script executions and interface systems (e.g. CLI and WebCI).

The Dynamic Configuration feature enhances the SDM platform by adding these new capabilities:

- Dynamic system configuration management
- Scalable cluster configuration
- Multi-node dispatching mode support
- Improved system startup and monitoring

Dynamic System configuration management

In the previous releases of the system, the system configuration was stored in a static configuration file (i.e., /blue/etc/default/SystemModel.xml). The SystemModel.xml still exists but its content is reduced to a limited set of mandatory entities. The concept of static and dynamic entities is added in order to categorize system model entities that must (static) be configured from one that could (dynamic) be configured in SystemModel.xml. With the dynamic configuration, the operator's system administrator is able to add service dynamically on a blade without having to deal with static configurations.

Dynamic entities

Here is the list of entities that can be configured dynamically by operator:

- SmModule (Adding a service to a slot adds a specific set of SmModule to this slot)
- Slot Identity (identity bind to a specific slot and that defines the basic set of services running on that slot)
- ServiceInstance (deployment of a service on a specific slot)
- ServiceInstanceOption (option specific to an instance of a service)

Refer to *Services Running on the System* in this document for a detailed description of the different services that can be supported by the system.

Scalable cluster configuration

With the scalability project, the system can support multi-nodes. Each service can regroup multiple instances that run on different blades of the system. A service group's instances form a cluster, which follows a specific redundancy policy, refer to *Services Running on the System* for more details on the different redundancy models supported by the system.

Protection redundancy modes are applied on a service basis, more precisely, if one of the User Services fails on a slot, it does not affect the Core Service or any other User Services running on that same slot. Only that User Service stops providing service and running traffic, but the other services running on that slot continue providing services.

This increases the system's scalability and performance.

Dependencies between the system's different modules also affect the state in which the services' instances run. Whenever any module fails on a service instance, the whole service instance fails. In addition, all user services (ex:Hlr service or Hss service) depends on the slot core service. It means that in order to add a user service to a slot, the CoreSystemController or CoreServiceNode service must be at least bind first. If the slot core service fails, all services on the slot will fail. But if a user service fails, only this service will fail.

Improved Traces

This feature brings improvements to the logging of the following system's events:

- Trace
- Trace Error

All of the events with Trace and Trace Error levels are called traces.

The improvements implemented in the system offer more flexibility and minimize the use of the system's resources and overall offer a better way for Tekelec's *Customer Care Center* to manage traces and perform troubleshooting.

WARNING: The operations implemented as part of the system's trace improvements and that are described below have been strictly implemented for the Tekelec's *Customer Care Center* and must not under any circumstances be performed by the operator. Traces are only useful during troubleshooting before which the Tekelec *Customer Care Center* must always be contacted.

Here are the improvements brought to the system's traces:

Traces are now written and stored locally where they are produced. Since the traces are no longer stored on the active and standby SystemControllers, the trace HA behavior for synchronization is no longer needed, thus significantly improving the system resource usage. The traces are stored locally on the blade (under /blue/var/trace) where the application concerned is running. The trace file name includes the time of the last trace in the file. The traces are stored in a set of files per process with a rotation schedule. The rotation is based on the maximum number of trace files, which are 100. The oldest trace file will be replaced with the newest file. Each trace file can contain up to 50000 trace lines. The system's other events with the following levels remain stored on the SystemControllers: Info, Notice, Warning, Error, Critical, Alert, Emergency and Alarm level.

The Traces are stored in a text format. Additional information about the component is included in the traces. A trace includes the following information:

- Time:

  This is the local time in format "Tue Nov 11 2008 09:44:49:530489 (microseconds)".
- Level:

  This is the event level or also called severity.
- File:

  This is the originating source file name.
- Line:

  This is the originating ling number in the source file.
- Slot Identification:

  This is the chassis slot identification
- Thread:

  The thread identification within the process
- Module:

  The Module name (extracted from the Module Identity)

- Component:

  This is an optional trace parameter used for filtering.

- Description:

  This is the text that is given with the trace.

The system offers the Tekelec *Customer Care Center* the ability to activate/deactivate traces for each module (i.e., process) of the system. This allows the Tekelec technicians to display or not a module's traces by executing through the CLI either one of the two following operations implemented: StartTrace(), StopTrace(). When the trace is activated for a module, all the log events (i.e. from Info level and up) are also stored in the trace file of that module. This helps to correlate events that occurred in time line by ordering all the events in one file.

The system also offers the Tekelec *Customer Care Center* the ability to filter on components for a given module's traces (i.e., process). With this filtering option, only specific traces can be displayed rather than the set of traces available for that process. By default, when activating the traces for a given module, all traces are produced. In order to reduce the number of traces produced, the Tekelec technicians can add filter specific components so that only traces about these components will be produced. Filtered Traces are activated per module (for the entire process) and by component. A list of filter specific components is predefined in the system for each module type. The following two operations can be executed by the Tekelec technicians in order to perform such filtering:

- AddFilterComponent ()
- RemoveFilterComponent()

Maximum Provisioning Template Size Control

The purpose of this feature is to allow the client to control the disk space occupied by the provisioning template requests. The Command Template Loader tool loads template requests (in XML language) into the database to support subscriber provisioning with templates. A size restriction has been implemented for the template requests to prevent them from occupying too much disk space.

The "MaxTemplateSize" parameter has been added to the OampManager entity to allow the operator to set that size restriction by defining the maximum total size (in bytes) the template requests can reach. If this parameter is not provisioned or turned off, there is no size control restriction for provisioning templates.

In addition, a "ProvTemplateDiskSpace" entity has been implemented to allow the operator to view the disk space allocated in the database for the template requests .

The provisioning of the MaxTemplateSize parameter and "ProvTemplateDiskSpace" entity can both be done by the operator through the CLI or WebCI.

For more information on the "MaxTemplateSize" attribute and the TemplateSize entity, refer to the "*Oamp Manager"* section of the SDM Monitoring, Maintaining, Troubleshooting - Reference Manual. For step-by-step instructions on how to provision them, refer to the "Controlling the Provisioning Template size" section of the SDM Monitoring, Maintaining, Troubleshooting - User Guide.

Performance Management Improvement

With the Performance Management Improvement feature, fault notifications and performance monitoring are improved. Additional alarms and counters have been implemented on the system as well as a statistic file.

Fault notification (alarms) improvements:

- 14 new threshold alarms which cover utilization of CPU, memory, and IP network interfaces, per blade.

Performance monitoring (counters) improvements:

- 5 new counter areas: CPU load, process information, memory usage, disk IO operations and IP network interface utilization.

Statistics file:

- A statistic file containing these new counters is generated on a daily basis. This statistic file can be characterized as follows:
- It is produced into the blue/var/pm directory.
- It is generated every day at 12:00 am and contains all the counters of the day stored in the database.
- It is named according to the 3GPP TS 32.435 v7.2.0 standard, as follows:
    - AYYYYMMDD.000000_240000_BluesliceNetworks_OS-Critical-Resource.xml
    - Where 'A': Type
    - YYYYMMDD: Start date
    - 000000: Start time (HHMMshhmm)
    - 240000: End time
    - Tekelec: UniqueId
    - OS-Critical-Resource: job name

The file is in an XML format, as per the 3GPP TS 32.435 v7.2.0 standard.

For the description on the added counters for the performance monitoring improvements, refer to the SDM Performance Measurements document. For the description on the added alarms for the fault notification improvements, refer to the SDM Alarm Dictionary document.

CPU Usage Monitoring

With this new feature, the SDM system monitors the CPU usage of each process by verifying the following:

- The CPU usage of each process every minute. If a process uses more than 95% CPU, the system verifies:
    - Each of the process's thread. If one given thread uses more than 95% of the CPU for 5 consecutive minutes, the system kills the process.

The purpose of the CPU Usage Monitoring feature is to prevent blade and traffic failure in case one application goes out of control and starts using all the processing power infinitely. If this happens, the process is killed and the following emergency alarm is raised:

- Alarm Name: "ProcessCpuLoad", Alarm Id="318"

Geo Redundancy

The SDM supports a geo-redundancy deployment architecture with a chassis located in two different sites with different time zones working in a master-to-master replication mode. Each site serves the

same subscriber base and is dimensioned to takeover the full traffic in case of a site failure. During normal operation each site processes traffic and actively maintains a database replica of the other.

The SDM follows the logic represented in the figures below to deploy geo-redundancy for the HLR and HSS services of the SDM.

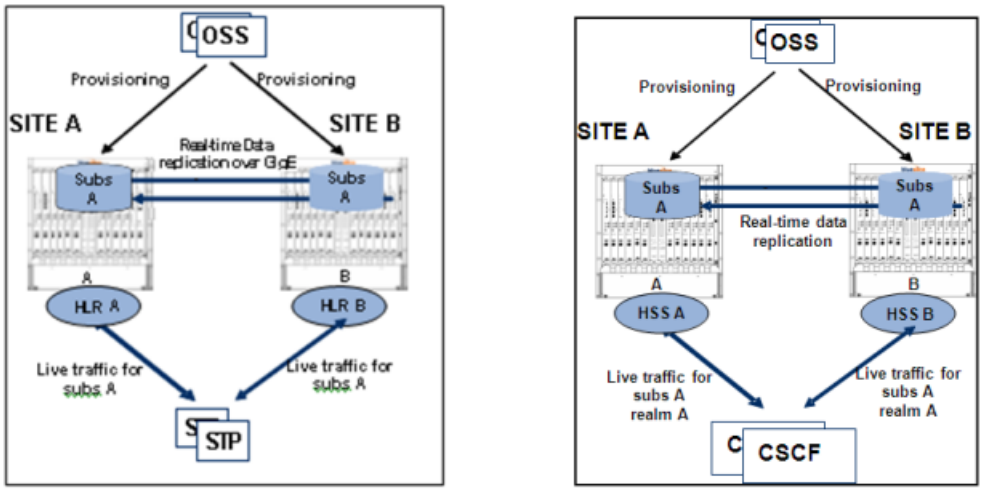


Figure 20: Geo Redundancy logic for the HLR and HSS services.

The software can be configured in two different ways.

- Geographic replication using replication link
- Geographic replication using IP Multi-homing

Hardware and Service configuration

The configuration of the SDM in a geo-redundant deployment is mostly done at installation. This is a list of the parameters defined during installation:

- The Geo-Redundancy feature is enabled.
- The identification of the database on each of the sites is defined.
- Each site is assigned a unique geo-redundancy virtual IP (VIP) address. The service provider's OSS system needs to be configured with the geo-redundancy VIP address of both sites.

Diameter peer nodes (e.g. a CSCF) which interact with the IMS-HSS are configured to connect to all IMS-HSS Diameter endpoints. For the Hss service, the hostnames and VIP used for Diameter are configured for each blade. The majority of the HSS service configuration is identical across all HSS service blades, for both sites. The exception is the HSS hostname and VIP used for Diameter; this must be unique for each blade. Furthermore, the VIP must be part of the network segment allocated to the public SDM IP addresses.

This is a list requirements to run the SDM in a geo-redundant deployment:

- Each site in a geo-redundancy deployment must be configured separately.
- Each site of a geo-redundant pair must be configured identically in a hardware perspective (e.g., if site A has 8 blades, site B must also be configured with 8 blades).

Once the SDM has been installed in a geo-redundant deployment, the operator can make these provisioning operations via the CLI or WebCI:

- The geo-redundancy VIP of the remote site and the state of the Geo-Redundancy feature (enabled or disabled) can be displayed.
- The geo-redundancy VIP of the remote site can be modified.
- The Geo-Redundancy feature can be disabled.

In the case where the connection between the two sites is lost, either due to the physical connection or the operational state of the other site, the state of the database changes. If the state of the database was in a replica state, it becomes in a PendingReference state and if it was in a ReferenceProtected state, it becomes in a Reference state. The operator can force the database to change from the PendingReference state to the Reference state.

If the geo-redundancy feature was disabled and later enabled once again or simply if the negotiating phase of the synchronization process could not determine which site has the reference database and which one has the replica database, the synchronization process would get into an unassigned state (UnassignedEnabled). To get out of this unassigned state, the operator must execute the resume operation, which will force the synchronization process to reenter the negotiating phase in order to identify which site has the reference database and which site has the replica database.

This table identifies the geo-redundant parameters used to configure the system along the their default values. Please refer to the *Geo-Cluster Configuration* section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual* to get more information about the provisioning parameters.

Table 6: Geo-Redundant Provisioning Parameters

Parameter	Description	Default Value
GeoClusterId	Id of the Geo cluster	0
GeoLocalSiteIp	Local virtual IP address of a site of type GeoReplication that works in a Geo-redundancy deployment	N/A
GeoLocalSiteNetmask	Netmask of the geo-redundant local site	N/A
GeoRemoteSiteIp	Virtual IP address of the peer site of type GeoReplication and with which it works with in a Geo-redundancy deployment	N/A
GeoRedundancyEnabled	Attribute that indicates if the Geo-Redundancy feature is enabled or not. 0=Disabled 1=Enabled	0

This table identifies the geo-redundant provisioning components and the location of additional information. Refer to the Geo-Cluster Configuration section of the *Viewing/Modifying the Information for a Geo-Redundant System* section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide* for step-by-step instructions on how to provision and modify the system in a Geo-redundant deployment.

Table 7: Reference Information

Affected Components	Description	Reference
Interfaces	CLI, WebCI	
Entities[], attributes	To Enable/Disable the Geo Redundant Information Display Geo Redundancy information Modify the Geo Redundancy Information Resume Geo-Redundancy Force the Geo Referencee	For WebCI refer to *SDM Monitoring, Maintaining, Troubleshooting User Guide*: • *Viewing/Modifying the Information for a Geo-Redundant System* For CLI refer to:*SDM Monitoring, Maintaining, Troubleshooting Reference Manual*: • *Geo-Cluster Configuration* • *Geo-Redundancy Operations*
Alarms	None	
Error Messages	None	

Geographic replication using replication link

In a Geo-Redundant deployment, the Data Provider Controller has the additional role of exchanging information with its peer by establishing direct connection using the public Geo-Redundancy Virtual IP address of the remote site. The Public Geo-Redundancy Virtual IP address is activated when the database service become active. Each site has its own Geo-Redundancy Virtual IP. The Geo-Redundancy VIP is re-activated on the new active on switchover events.

Once the connection between the two geo-redundant sites is established, the Data Provider Controller is in charge of managing the synchronization and replication between the main active database in a ReferenceProtected state and the main active database in a Replica state of the two sites geographically distributed. This exchange of information between the two sites is done through a master-to-master replication link. Moreover, the Data Provider Controller can manage successfully the synchronization and replication of the data between two sites even if they are located in different time zones. The database replicated between the two sites includes the subscriber profile and the service-specific volatile data. Every update applied against the database on a given site is replicated on the peer site.

The connection between the two geo-redundant sites can be lost in cases where:

1. There is a problem with the physical connection between the two sites.
2. There is a problem at one of the two sites. A database switchover on one site would cause the geolink to go down temporarily. A complete power failure at one site would cause the geolink to go down permanently.

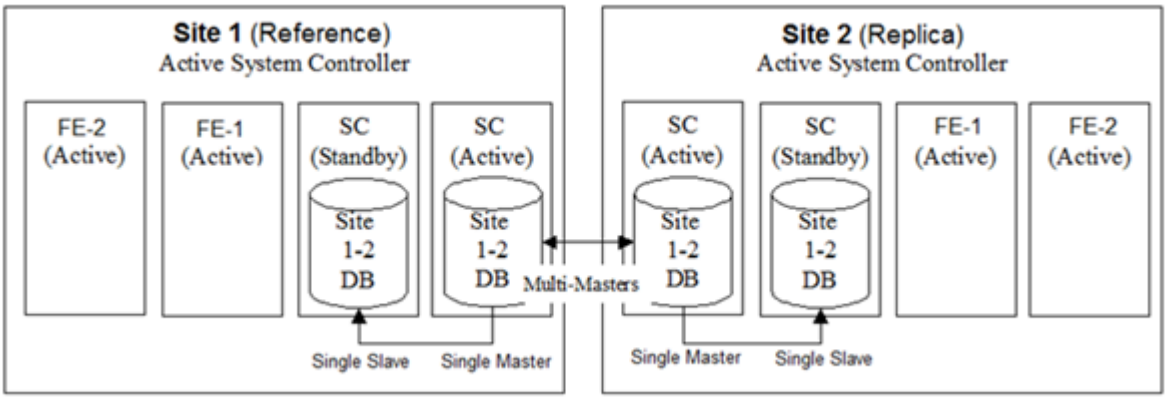


Figure 21: Data replication between two geo-redundant sites.

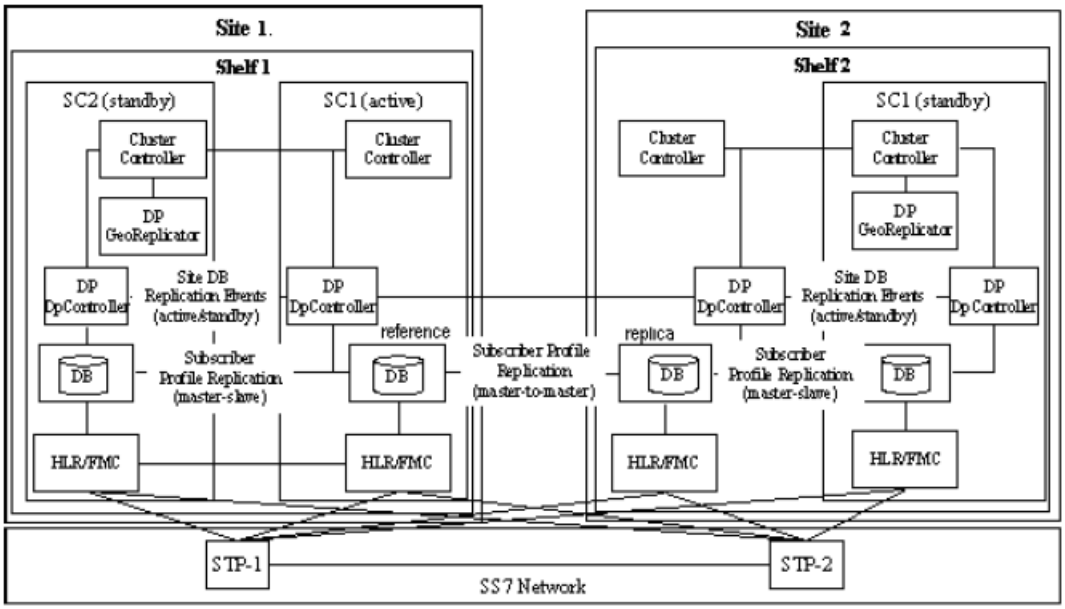


Figure 22: Data replication between two geo-redundant sites at the process level.

For the SDM with the Tekelec ngHLR product running in this type of geo-redundant deployment, there is no load-sharing functionality. Since there is one primary address to transport the traffic, each interface and network path must be dimensioned to support all the appropriate traffic with the desired performance characteristics.

For the SDM with the IMS-HSS product running in a geo-redundant deployment, the network connectivity must be respected as follows:

A unique hostname and VIP must be assigned to each HSS service blade in order to be used as a Diameter endpoint. A minimum of 2 Diameter endpoints per shelf ensures redundant HSS Diameter connectivity for one site.

For a geo-redundant deployment there is a minimum of 4 HSS service blades, all serving the same realm.

The facing Diameter peer (e.g. a CSCF) must be configured to use all 4 HSS Diameter endpoints. Should one site fail completely the CSCF remains connected to the surviving site - this provides redundancy for the Diameter realm.

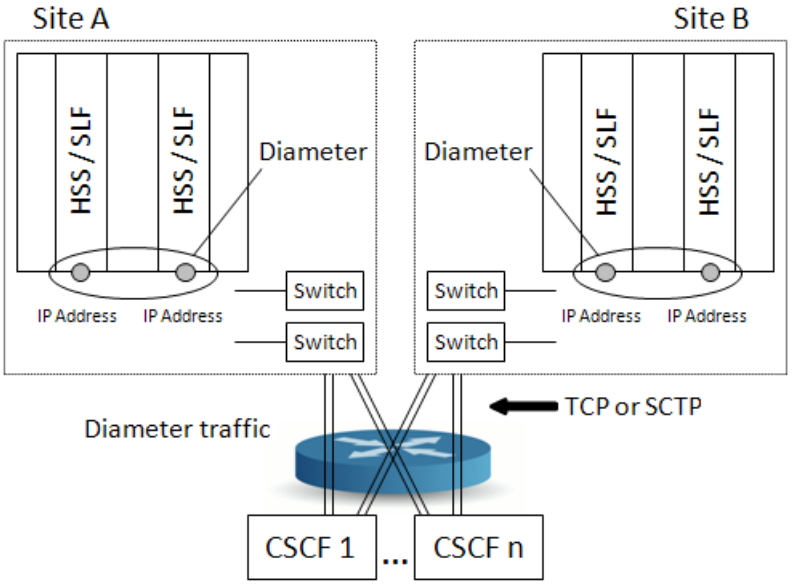


Figure 23: IMS-HSS network connections in a geo-redundant deployment.

For step-by-step instructions on how to configure each HSS service blade and assign them with a unique hostname and VIP, please refer to the "Configuring the HSS" section of the SDM System Configuration - User Guide.

For the SDM with the AAA product running in a geo-redundant deployment, the network connectivity must follow the following guidelines:

For each AAA endpoint configured on the SDM on Site A, a similar AAA endpoint to the same NAS(s) must also be configured on the SDM at Site B. This ensures that should one site fail completely, all connections to all NASs will be available on the geo-redundant site.

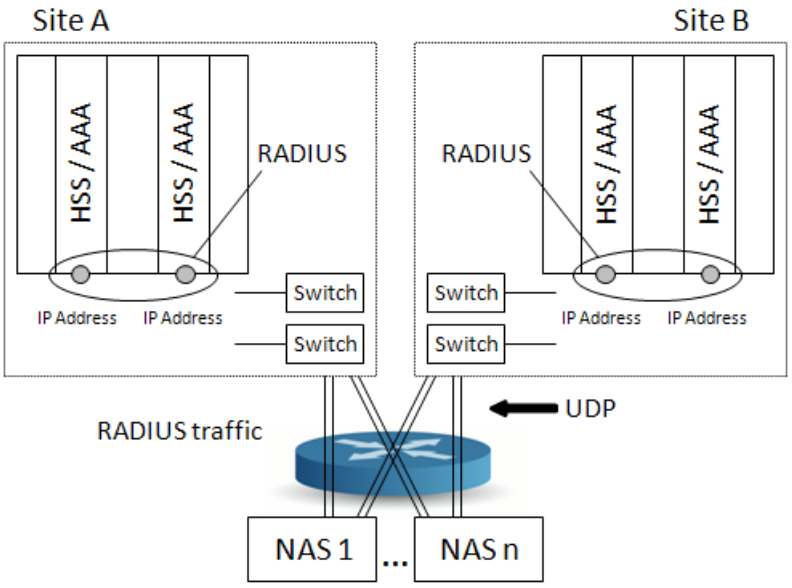


Figure 24: AAA network connections in a geo-redundant deployment.

Geographic Replication Using IP Multi-Homing IP Addresses

This feature uses an IP tunnel (IP network communications channel between two networks) between the SDM Active System Controllers (backends) to transport geo-redundancy traffic. The IP tunnel is maintained by software on each controller. Multiple IP addresses on each side and the SCTP are used to transport data between tunnel endpoints. This Multi-homing technique is used to increase reliability of IP communications across several IP networks.

The geographic replication feature addresses problems arising from real-time subscriber database systems in which more than one database instance can accept "write" transactions and cause conductivity to become unavailable.

This feature prevents the end-to-end Subscriber Data Server (SDS) system from entering into a "split-brain" situation. In this situation there would be an outdated response to the SRI on a second site and a failed call or SMS.

All geo-redundancy traffic is transported through the tunnel, including:

- SDM geo-redundancy control traffic
- Database backups transferred via SCP (using the SSH protocol)
- Tungsten Replication MySQL engine connections

All three ways use TCP/IP communication, so the tunnel can be limited to IP communication only (layer 3).

This figure provides a high-level graphic summary of multi-homed IP tunneling.

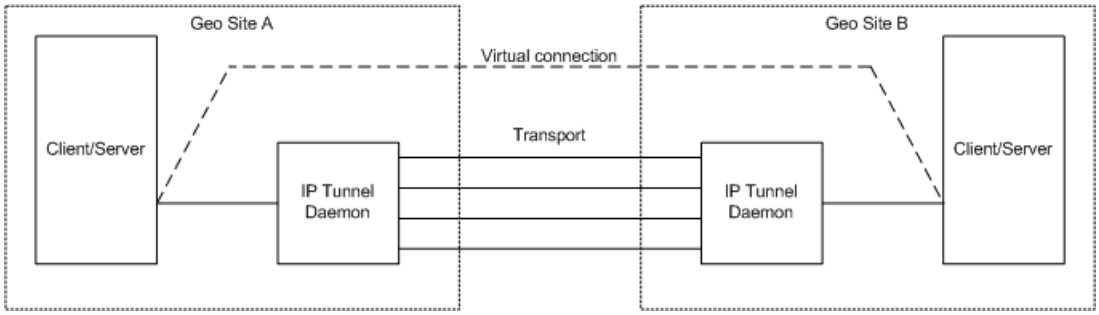


Figure 25: Multi-Homed IP Tunneling

The SCTP/IP stack supports IP multi-homing to maintain the tunnel over the SCTP. Selected traffic is intercepted for tunnel transport and re-injected (after tunnel transport) into traffic applications. Selection of which IP traffic goes over tunnel transport is done using the IP routing tables, where traffic that is tunnel-bound is routed to a virtual "tunnel" interface.

The software works in client/server mode to make the SCTP connection establishment simpler.

There is no restriction on the number of interfaces to use, but it is recommended that more than one physical interface be used to keep the tunnel up in the event that an interface is experiencing problems.

There is no load-sharing functionality with this feature. Since the SCTP selects one primary address to transport the traffic, each interface and network path must be dimensioned to support all the appropriate traffic with the desired performance characteristics.

The multi-homed geo-redundancy feature works on any existing IP network interface that is supported by TPD Linux and SDM for a given SDM-supported hardware platform.

Counters

Counters are available upon request and when the system is stopped. The counters include all packet/bytes that are transported/dropped by the tunnel. The system counters for the TUN interface and the SCTP association are also available. Counters are output to log files.

Note: Only users with admin privileges are allowed to execute this script.

Table 8: Available Counters

script	Command	Description	Output location
sdm-geored-tun-cli	`get-counters`	Request the output of the counter values in the log	`/var/log/messages`
	`clear-counters`	Clear the counter values	`/var/log/messages`
	`ifconfig tun` x	Displays information about the TUN interface	`/proc/net/sctp/snmp`
	`ifconfig sctp` x	Displays information about the SCTP association	`/proc/net/sctp/snmp`

Feature Activation

This feature is automatically be enabled when the file `/etc/sysconfig/sdm-geored-multihome.conf` is present, and when the Local SiteVip is the

same as the configured `SDM_GEORED_VIP`. These files are configured by Tekelec Customer Support during installation and cannot be modified by the customer.

When the Multi-Homing Geo-Redundancy feature has been configured/enabled on an SDM system, processing of the activation of a local geo-redundancy VIP is modified to include these additional actions:

- Activation of several additional VIPs (typically a minimum of 2 but can be more) intended for use in SCTP transport
- Creation of extra IP routes (this is driven by VIP activation through sdm-vlans.conf configuration as documented in REF
- Startup of the geored tunneling daemon (which creates the tunnel interface and sets up the SCTP association with the remote peer)

The software will start, and once started the software is monitored using `Monit::Monitor`.

Subscriber Provisioning

Since each site serves the same subscriber base and since all subscriber profile changes are replicated on both sites, OSS subscriber provisioning may be done via either site or even in a distributed manner by load-sharing the subscriber provisioning traffic across both sites. In the latter case, the traffic distribution is the responsibility of the service provider's OSS system.

Backups of subscriber profile data and service volatile data may be taken on either site and may be restored on either site. Restoring one site does not impact all the other sites.

The subscriber provisioning for a SDM in a geo-redundant deployment can be done from either site using the CLI or WebCI. For step-by-step procedures on how to provision subscribers through the WebCI and CLI, please refer to the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*. For information and examples on how to provision subscribers using the XML language, please refer to the *SDM Subscriber Provisioning - User Guide and Reference Manual*. For instructions on how to perform backups of the database in a Geo-Redundant deployment, refer to the *Troubleshooting a Geo-Redundant system - Backup/Restore Procedures* section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Multi-Profile representation in the WebCI

The graphical interface (WebCI), used to display subscriber profile information, is modified in the SDM. All folders in the WebCI related to subscriber provisioning are moved from their respective application to a new separate folder " Subscriber Management ". The new folder provides access to a new unified subscriber view, providing access to all types of profiles associated to a subscriber (HLR, IMS-HSS, AAA, SIP) through a single window.

Self Healing

The SDM system has an internal replication mechanism that synchronizes the data between each of its servers. In order to make the replication more robust, a database monitoring automation process called Database Replication Monitoring (DRM) has been implemented. The DRM's main objectives are:

- To detect and log database schema out-of-sync(OOS)
- To detect and log data out-of-sync(OOS)
- To provide correction to data OOS and log all the corrections

- To provide indication (via alarms) to user interface all the schema discrepancies which can't be corrected or need manual correction.
- To provide module option control, such as: monitoring time (when), monitoring period (how often), monitoring length (how long), enable/disable, etc.

The DRM process runs within the Database service, which runs in Active/Standby mode on both System Controller blades. Only the one that runs with the master database server (i.e. active) will actually monitor the replication robustness. For details on the configuration for a Geo-Redundant deployment, refer to the "Self Healing (Database Replication Monitoring" section of the *SDM System Configuration - Reference Manual*.

The DRM produces report files to log all the discrepancies that are found and all the corrections done or that can't be done. The Network Operator can analyze these reports and send it to the Tekelec *Customer Care Center* if anomalies are detected.

These report files are saved in both System Controllers under the following directory: /blue/var/drm , with the name defined in the following format:
`<Database>-<Host>-<Operation>-<Timestamp>.txt`

- Database:

  Represents the database's name which is monitored (such as: bluedb , bluedbvol , etc.).
- Host:

  The slave database IP address. In format: 255.255.255.255
- Operation:

  The schema check, data check (i.e. discrepancies detection) or data sync (i.e. discrepancies correction).
- Operation:

  The schema check, data check (i.e. discrepancies detection) or data sync (i.e. discrepancies correction).
- Timestamp:

  Represents the time when the DRM file is created and has the format yyyymmddhhmmss.

The DRM supports report file rotation. Up to one hundred monitoring report files are kept under the drm directory. Note that even though the DRM report is generated by the active DRM process, the report is also copied to the System Controller standby. In a Geo system, the report will be kept in the **reference** system.

The discrepancies found on the database structure **will not be corrected** by the DRM process, but will be flagged by an alarm and will be stored in the DRM report. The alarm is defined as:

Table 9: DRM critical alarm

Severity	Description	Effect	Required Action
Critical	Database schema out-of-sync with <Slave DB IP> on <database>.<table>	Data inconsistent	Contact Tekelec's *Customer Care Center*.

The schema differences will be stored in the report with the following information:

Table 10: DRM report

Field	Description
Slave host	Slave DB IP
Master host	Master DB IP
Database	Name of database which has discrepancies
Table	Name of table which has discrepancies
Field	Name of field which has discrepancies
Constraint	Name of constraint which has discrepancies
Index	Name of index which has discrepancies
Trigger	Name of trigger which has discrepancies
Description	Describe the difference

The following shows an example of a report:

```
Differences on slave=169.254.1.13, master=192.254.1.12
TYPE          CONTEXT                                    DESC
Field         blueoam.oamdatabase.DbStatus               Added
Trigger       bluedb.hlrspcallbarringog_bsg.cb_1         Deleted
```

The Network Operator can configure and control the DRM process's following characteristics by configuring the DrmConfig[] entity through one of the available user's interfaces (CLI, WebCI, SOAP, CmdFileLoader): activation status, monitoring mode, monitoring time, monitoring period, monitoring method and the action the DRM must take when discrepancies are encountered (re-synchronize or print out differences).

For more details on the DrmConfig[ ] entity , refer to the "Self Healing (Database Replication Monitoring) " section of the SDM System Configuration - Reference Manual . For instructions on how to configure/control the DRM process from the WebCI, refer to the "Viewing/Modifying Database Replication Monitoring (DRM) configuration" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Stream Control Transmission Protocol (SCTP)

The SDM system supports SCTP over SIGTRAN and Diameter in order to carry call control signals in IP networks. It supports the following SCTP features:

- SCTP Multi-homing
- SCTP Multi-streaming

The next sections describe these SCTP features in more details.

SCTP Multi-homing

The system supports both the SCTP single homing and Multihoming (multi-homed SCTP session) capabilities. By default, both capabilities are enabled on the system for the HLR's Sigtran protocol and for the IMS HSS and LTE HSS's Diameter protocol.

The Tekelec ngHLR's SS7 stack and the IMS HSS and LTE HSS's Diameter stack all use the Kernel SCTP interface. This allows the HLR, IMS HSS and LTE HSS applications to run simultaneously on

the same blade within the same SDM platform. A Linux/SCTP stack, which is pre-compiled within the Operating System's kernel, is used for the SCTP protocol. The M3UA interfaces with an implementation of TUCL that uses the LKSCTP library to communicate with the Kernel SCTP.

The SCTP Multihoming functionality secures the local access by offering redundant LANs, hence preventing any temporary unavailability of transport. This adds more robustness to the SDM system and ensures the SCTP associations to become tolerant against physical network failures. This means that the Network Operator can configure the SCTP protocol with different local/destination IP addresses and different routes in order to make the SS7/Diameter traffic travel from one node to another on different physical paths, through different networks. As per the RFC 3286 standard, one single address is chosen as the "primary" address and is used as the destination for all data packets for a normal transmission. In case of partial or complete failure to send packets to the "primary" address, some or all data packets will be re-transmitted using the alternate address(es). This increases the chances of all the data to reach the remote endpoint correctly without any interruptions.

Note that SIGTRAN/Diameter will stay connected if there is at least one remaining SCTP connection (local and peer). Alternatively, should a failure occur on the SCTP connection, the system would try to reconnect to the peer node if the SDM system's ngHLR is the client of the association and in the case of the IMS-HSS and LTE-HSS, if the AutomaticPeerReconnect configuration parameter is enabled (set to '1').

Take note that a single port number is used across the entire list of IP addresses for a specific SCTP session.

The following table lists SCTP parameters configured in the system along with their default values.

SCTP Parameter	Description	Default Value
RTO Min	Minimum value for retransmission timeout	1000 ms
RTO Max	Maximum value for a retransmission timeout	60000 ms
RTO Initial	Initial value for a retransmission timeout	3000 ms
Max Init Retrans	Maximum number of times an INIT chunk or a COOKIE ECHO chunk is retransmitted before an endpoint aborts the initialization process and closes the association	8
Path Max Retrans	Maximum number of consecutive retransmissions to a particular destination address before marking it inactive	5
HB interval	Used in combination with the current RTO to schedule when the next HEARTBEAT chunk will be sent to an idle destination address	30000 ms
sack_timeout	Delayed SACK timeout	200 ms

Diameter

The SDM's IMS-HSS and LTE-HSS applications support SCTP multi-homing over Diameter.

From any of the system's provisioning interfaces, the Network Operator can define one single or multiple TCP/SCTP local/destination IP address(es) in the IMS HSS and LTE HSS's configuration entities. Take note that the system's default listen connection is on the TCP transport protocol. The local ports are pre-configured as follows:

- Local TCP Port:3868
- Local SCTP Port:3869

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 11: Provisioning Information - Diameter over SCTP Multi-homing

Affected Components	Description	Reference
Provisioning Interfaces	CLI, XML, XML-SOAP, WebCI	
Entities[], attributes	To enable/disable the SCTP transport protocol and the Automatic Peer Reconnect capability: • For the IMS-HSS: HssConfig[], SCTPTransport, AutomaticPeerReconnect • For the LTE-HSS: LteHssConfig[], SCTPTransport, AutomaticPeerReconnect To define the list of SCTP local/destination IP address(es): • For the IMS HSS: HssConfigSCTPListenAddress[] • For the LTE HSS: LteHssConfigSCTPListenAddress[]	*SDM Subscriber Configuration Reference Manual*: • *HSS Configuration* • *LTE-HSS Configuration*
Alarms	None	---
Error Messages	None	---
Counters	None	---
Procedures	• *Configuring the IMS-HSS/SLF* • *Configuring the LTE-HSS*	*SDM System Configuration User Guide Manual*: • *IMS-HSS/SLF Application Configuration* • *LTE-HSS Application Configuration*

SIGTRAN

The SDM's HLR application supports SCTP multi-homing over SIGTRAN.

From any of the system's provisioning interfaces, the Network Operator can define one single or multiple SCTP remote IP address(es) and provision the local and remote ports in the HLR SIGTRAN's M3UA SCTSap.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 12: Provisioning Information - SIGTRAN over SCTP Multi-homing

Affected Components	Description	Reference
Provisioning Interfaces	CLI, XML, XML-SOAP, WebCI	
Entities[], attributes	To define the list of SCTP remote IP address(es): • RemoteAddresses[] To provision the local and remote ports: from the HLR M3UA SCT Sap: • PSP[] The local port is configurable, but note that it should be different than the other SCTP user value (i.e., different than the Diameter port). According to RFC 4666, the recommended value for the local and remote port is 2905.	*SDM Subscriber Configuration Reference Manual*: • *PSP*
Alarms	None	---
Error Messages	None	---
Counters	None	---
Procedures	• *Configuring the PSP*	*SDM System Configuration User Guide Manual*: • *Configuring the SS7 stack using the TUCL, M3UA protocols (SIGTRAN)*

SCTP Multi-streaming

The SDM system also supports the SCTP Multi-streaming feature, which allows multiple simultaneous data streams per connection or association. The system can send multiple messages simultaneously

with each a different final destination. When using multi-streaming, one message must be sent completely through the same stream. By default, the SDM system always uses the multi-streaming feature for SCTP. This ensures a higher performance and overall higher capacity of the system. Using SCTP Multi-streaming has many benefits, such as the following:

- In "Head-of-Line Blocking" scenarios (When running an ordered data delivery system, if one of the packets is out of order or missing, the stream is blocked pending resolution to the order), the use of multi-streams would isolate the blocking issue only on the stream that is affected and the other streams would continue to flow.
- Reduce overall latency by allowing to process different types of data (voice, text, pictures, video, etc.) simultaneously.
- Simplify connectivity. Reduce overhead on servers due to numerous separate connections often required to process a request.

The SDM system supports the following number of streams:

- Over Diameter: the SCTP associations support eight incoming SCTP streams and eight outgoing SCTP streams.
- Over SIGTRAN: the SCTP associations have by default ten streams and the maximum number of streams supported is one hundred. Note that the number of streams supported may vary and is negotiated during the association establishment.

Tekelec ngHLR Features

The Mobile Application Part-GSM (MAP-GSM) supports interactive mobile applications (e.g., cellular, paging, voice messaging) between the network switching elements in a GSM system. These elements include Home Location Registers (HLRs), Visitor Location Registers (VLRs), Mobile Switching Centers (MSCs), Serving GPRS Support Node (SGSN), and so on.

The MAP is used by the Mobile Switching Center (MSC), Serving GPRS Support Node (SGSN), and Gateway GPRS Support Node (GGSN) in wireless networks to query the Home Location Register (HLR) or Visitor Location Register (VLR) to determine and/or verify subscriber services.

The MAP-GSM features supported by the SDM are listed below. These features are detailed in the 3GPP TS 29.002 version 4.11.0 Release 4: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile Application Part (MAP) specification" as follows.

Tekelec ngHLR 3GPP standard features

Mobility features

Location management

- Location Updating

  This service is used by the VLR to update location information stored in the HLR.

- Location Cancellation

  This service is used between the HLR and VLR to delete subscriber's records from the VLR.

- Purge MS

This service is used between VLR and HLR and SGSN and HLR to mark the MS in HLR database as not reachable.

- Update GPRS Location

  This service is used by the SGSN to update the GPRS location information stored in the HLR.

Fault recovery procedure

- Reset

  This service is used by the HLR, after a restart, to indicate to a list of VLRs or SGSNs that a failure occurred.

- Forward check ss indication

  This service may be used by an HLR as an implementation option, to indicate to a mobile subscriber that supplementary services parameters may have been altered, e.g. due to a restart. If received from the HLR, the VLR shall forward this indication to the MSC, which in turn forwards it to the MS. The HLR only sends this indication after successful completion of the subscriber data retrieval from HLR to VLR that ran embedded in a MAP_UPDATE_LOCATION procedure.

- Restore data

  This service is invoked by the VLR on receipt of a MAP_PROVIDE_ROAMING_NUMBER indication for an unknown IMSI, or for a known IMSI with the indicator "Confirmed by HLR" set to "Not confirmed". The service is used to update the LMSI in the HLR, if provided, and to request the HLR to send all data to the VLR that are to be stored in the subscriber's IMSI record.

Macro Insert_Subs_Data_Framed_HLR

This macro is used by any procedure invoked in HLR which requires the transfer of subscriber data by means of the InsertSubscriberData operation (e.g. Update Location or Restore Data).

Authentication management services

- Send Authentication Info

  This service is used between the VLR and the HLR for the VLR to retrieve authentication information from the HLR.

- Authentication Failure Report

  This service is used between the VLR and the HLR or between the SGSN or HLR for reporting of authentication failures.

Operation and maintenance features

- Subscriber data management
  - Subscriber deletion procedure (SGSN supported).

    The cancel procedure can also be triggered by the HLR to delete a subscriber record in a previous VLR.

  - Subscriber data modification procedure (SGSN supported).

    In the subscriber data modification procedure the subscriber data is modified in the HLR and when necessary also in the VLR or in the SGSN.

- Subscriber identity procedure

Call handling features

- Send Routing Information.

  This is used between the Gateway MSC and the HLR to interrogate HLR in order to route the call to the terminating MS.

- Provide Roaming Number.

  This is used between the HLR and VLR to request a roaming number from the VLR in order to route a call to the terminating MS.

SRI-LCS According to 3GPP R6 LBS

This feature provides the Tekelec ngHLR the capability to support the MAP SRI-LCS service (Location-Based-Services ((LBS)) within compliance of the 3GPP Rel.6 Location-Based Services (as per the 3GPP TS 29.002, VERSION 6.17.0, Release 6, July 2010 and as per the 3GPP TS23.271, version 6.13.0, Release 6, September 2005). This service is used between the GMLC and the Tekelec ngHLR to retrieve the routing information needed for routing a location service request to the servicing VMSC or SGSN.

This feature allows the Tekelec ngHLR to accept a Send Routing Info for LCS (SRI-LCS) message from a GMLC and respond to it appropriately. The SRI-LCS message includes an MLC number and MSISDN or IMSI. The Tekelec ngHLR retrieves the routing information of the subscriber and then responds with the Send Routing Info for LCS Ack message.

With the implementation of this feature, the Tekelec ngHLR offers the following capabilities:

- Receiving LCS data from a VLR and storing it in the volatile data for the subscriber.
- Receiving LCS data from an SGSN and storing it in the volatile data for the subscriber.
- Sending to a GMLC the LCS data provided by the VLR and/or serving SGSN.
- Provisioning a list of H-GMLC and PPR addresses for each PLMN.
- Sending to a GMLC the provisioned H-GMLC and PPR addresses.
- Sending to the VLR or serving SGSN the list of provisioned H-GMLC addresses.
- Deleting from the VLR or serving SGSN the list of GMLC addresses allowed to perform a location request for the subscriber.
- Provisioning an LCS privacy profile for each subscriber. A subset of the privacy profile is supported, including the following LCS privacy exception classes:
  - Universal class
  - PLMN operator class
- Sending the LCS privacy profile of the subscriber to the VLR or serving SGSN.

SRI-LCS message handling

The Tekelec ngHLR is part of the Mobile-Terminated Location Request (MT-LR) message flow defined in section 9.1.1 of the 3GPP TS23.271, revision 6.13.0, R6, September 2005.

This figure shows the common message flow for the MT-LR.

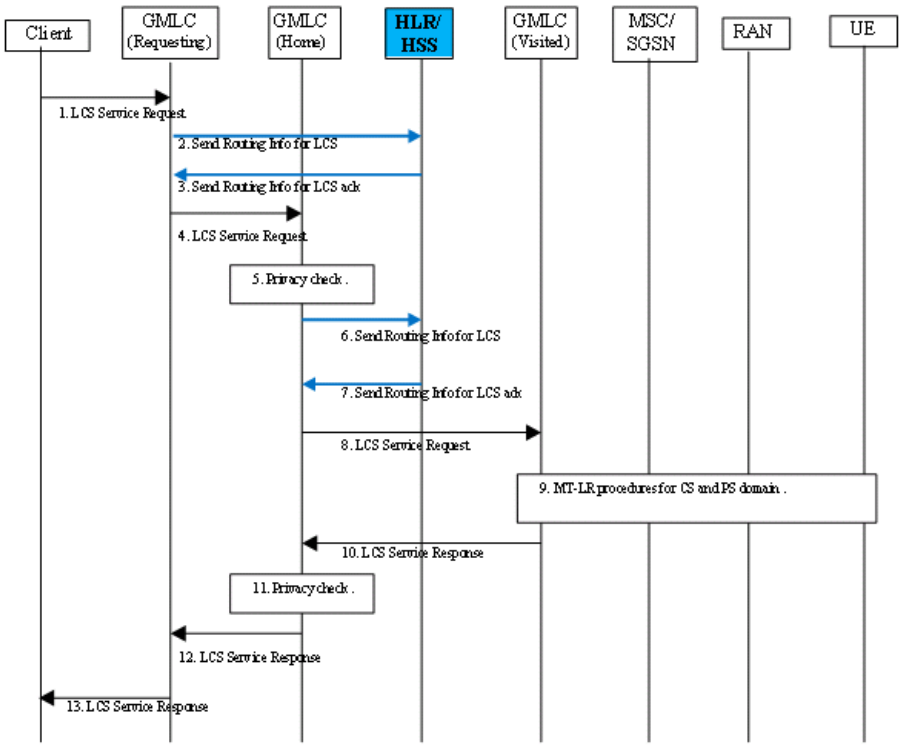


Figure 26: SRI-LCS Call Flow

The interaction of GMLC with the Tekelec ngHLR gives the following added benefits with regards to the MT-LR:

- A Requesting GMLC *(*R-GMLC*)*can obtain the LCS capabilities of the VLR or serving *SGSN*, and therefore decide whether and where to send a location request.
- A R-GMLC can obtain the*H-GMLC* and V-GMLC addresses. The R-GMLC may forward the location request to the H-GMLC if a privacy check is required, including the V-GMLC address. The H-GMLC performs a privacy profile check, and if the check passes, the location request is further forwarded to the V-GMLC. In some cases, such as emergency location requests, an R-GMLC may also send the request directly to the V-GMLC.
- A H-GMLC can obtain the *PPR* address, in cases where the PPR is not co-located with the H-GMLC.
- The LCS privacy profile stored in the ngHLR can be uploaded to the VLR and serving SGSN, to enable these network elements to screen location requests (PROVIDE-SUBSCRIBER-LOCATION).

The Tekelec ngHLR is not directly involved with the Mobile-Originated Location Request (MO-LR), but it is responsible for uploading any MO-LR privacy profile settings to the VLR/SGSN.

Note: The Tekelec ngHLR does not support MO-LR privacy profile. Only the MSISDN, IMSI, LMSI, NetworkNodeNumber, GPRSNodeIndicator, and AdditionalNumber parameters are supported in a successful response.

SRI-LCS Process

The Tekelec ngHLR processes the SRI-LCS message as per the 3GPP standard, with the following extensions/variations and assumptions:

- A SRILCSAllowed parameter has been implemented in the SubscriberProfile table in order to allow the Network Operator to enable/disable the SRI-LCS processing on a per subscriber basis. By default, the SRI-LCS is always enabled. This means the Tekelec ngHLR will process the SRI-LCS message normally, as per the 3GPP R6 LCS standard. However, if the Network Operator has disabled the SRI-LCS by setting the SRILCSAllowed parameter to false (0), the Tekelec ngHLR will return a MAP error of Facility Not Supported. (See *Subscriber Provisioning Reference Manual* for more information on setting this parameter.)
- SRI-LCS response prioritization supports the parameters "`CS LCS Not Supported by UE (CSLCSNotSupByUE)`" and `PS LCS Not Supported by UE (PSLCSNOTSupByUE)` flags in the volatile data table that dictates whether to send the serving MSC or serving SGSN address in the `networkNode-Number` parameter of the SRI-LCS response. These parameters are used in cases where the UE is registered both as GSM and GPRS. In these cases, the address sent in the `networkNode-Number` is the address that the GMLC uses as a priority over that sent in the `additionalNumber`.

  The prioritization is shown in this table.

CS LCS Not Supported by UE	PS LCS Not Supported by UE	NetworkNode Number	Additional Number	Description
False	False	MSC number	SGSN number	There is no guidance in these standards for this case. The Tekelec ngHLR recommends the MSC number to be sued in priority over the SGSN number as an implementation-specific decision.
True	False	SGSN number	MSC number	
False	True	MSC number	SGSN number	
True	True	MSC number	SGSN number	There is no guidance in the standards for this case. Tekelec ngHLR returns both addresses and allows the SRI-LCS to complete despite the fact that neither CS or PS location requests are supported and allows the GMLC to try a location request, although it is possible that it may fail anyway. **Note:** This is an implementation-specific decision.

  (See *Subscriber Provisioning Reference Manual* and the *Monitoring Maintenance, Troubleshooting User Guide* for more information on enhancements to the VolatileProvisioning table.)

- No LCS support if VLR uses MAP version1 or 2

  If the VLR uses MAP version 1 or 2 for the UPDATE-LOCATION message, then it is assumed that the VLR and MSC do not support LCS at all. It is technically possible that the MSC in fact supports PROVIDE-SUBSCRIBER-LOCATION (using MAP version 3), despite the VLR using MAP version 1 or 2 in the UPDATE-LOCATION. However, this is considered unlikely. This assumption also

simplifies the procedure for INSERT-SUBSCRIBER-DATA, such that the LCS Information parameter is omitted for INSERT-SUBSCRIBER-DATA sent in response to UPDATE-LOCATION using MAP version 1 and 2.

- Duplication of LCS SS-Code and SS-Status in SS-Data-List and LCS Information MAP parameters

  Duplicating the LCS SS-Codes in these parameters shall not be treated as an error. Therefore the assumption is made that the SS-Codes corresponding to LCS privacy classes (and their SS-Statuses) must be included at same time in the SS-Data-List and LCS Information parameters.

- Deprovisioning of LMU identifier may require a manual CANCEL-LOCATION

  When the LMU indicator is de-provisioned for a subscriber, the HLR does not notify the VLR of the change. There does not appear to be any method to achieve this using DELETE-SUBSCRIBER-DATA. Therefore a manual CANCEL-LOCATION is required in this case.

This table shows a summary of possible SRI-LCS Processing results:

Table 13: SRI-LCS Message Handling

DB Lookup Result	SRI-LCS Processing Result
Subscriber is not provisioned	`Unknown Subscriber` error
Subscriber is provisioned, but not reachable	`Absent Subscriber` error
Subscriber is provisioned and reachable via GSM and/or GPRS	`Send Routing Info for LCS Ack` Included in this response is the MSC number and/or SGSN number in the NetworkNode-Number and AdditionalNumber parameters. **Note:** In the case of dual-mode registration (GSM and GPRS), the MSC number is always returned in the NetworkNode-Number parameter and the SGSN number in the AdditionalNumber parameter
Error accessing the database	`Unknown Subscriber` error

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 14: Provisioning Information - SRI LCS

Affected Components	Description	Reference
Provisioning Interfaces	CLI, WebCI, XML interfaces: XML	

Affected Components	Description	Reference
Tables[]/ attributes	• To enable/disable the support of the SRI LCS messages on a per subscriber-basis, provision the SRILCSAllowed attribute in the Subscriber Profile[] table.	*SDM Subscriber Provisioning Reference Manual:* • *Subscriber Profile (Bearer Services, Teleservices, Call Barring, PerferredRouting NetworkDomain)*
	• To define LCS privacy exceptions provision the LCSPrivacyException[] List table, (for example, SSCode, SSStatus, InternalClient, NotificationToMsUser).	• *SDM Subscriber Provisioning Reference Manual:* • *LCS Privacy Exception List*
	• To define the Home PLMN provision the HPLMN[] table (for example, PPRAddress, HGMLCAddress).	*SDM System Configuration Reference Manual:* • *Home PLMN*
	• To display SRI LCS related data the system stores in the volatile data, display the HlrVolatileData[] table.	*SDM Subscriber Provisioning Reference Manual* • *Privacy Exception List*
Alarms	None	*Alarm Dictionary*
Error Messages	HPLMN-Trying to set Universal Class without at least setting one InternalClient-Error 5256	*SDM Monitoring, Maintaining, Troubleshooting Reference Manual*
Counters	None	*Performance Measurements*
Procedures	Provisioning a subscriber's LCS privacy profile • *Provisioning a subscriber HLR service profile*	*SDM Monitoring, Maintaining, Troubleshooting User Guide:* • *Provisioning a subscriber HLR service profile*

Affected Components	Description	Reference

	Provisioning and defining a subscriber's Home PLMN
	• *Provision HPLMN services*
	  • PPRAddress
	  • HGMLCAddress
		SDM System Configuration User Guide

	Provisioning a subscriber's profile for LCS • *Provision LCS services for a subscriber*	*SDM Subscriber Provisioning User Guide*
	Displaying SRI LCS related data the system stores in the HlrVolatileData[] table • *Displaying HLR Volatile Data*	*SDM Monitoring, Maintaining, Troubleshooting User Guide* • *Displaying HLR Volatile Data*

Supplementary Services

The Tekelec ngHLR supports supplementary services.

Advice of Charge (Information) (AoCI)

Definition

This service permits the mobile station (MS) to display an accurate estimate of the size of the bill which will eventually be levied in the Home PLMN.

Description

This supplementary service provides the MS with the information to produce an estimate of the cost of the service used. Charges are indicated for the call(s) in progress when mobile originated or for the roaming leg only when mobile terminated. Any charges for non-call related transactions, and for certain supplementary services, such as Call Forwarding are not indicated.

The MS will receive at the beginning of each call (and as necessary during the call) a message, the Charge Advice Information. This message contains the elements which together define the rate at which the call is to be charged, time dependence, data dependence and for unit increments.

The MS still indicates appropriate charges even when roaming based on Home PLMN units.

Where applicable, the volume charge for Packet data service, in addition to the normal time dependent and incremental charges, will be indicated.

To indicate the charge per call, the Mobile station shall display the units consumed so far during the present call(s) and maintain this value until the MS is switched off or a new call setup is attempted.

Where required to indicate the total accumulated charge, the MS displays, and the SIM stores in the ACM, the running cumulative unit charge. This value must be stored securely, and all reasonable

steps must be taken to ensure that the written value cannot be interrupted, reset or corrupted (except resetting under control of the unblocking key).

Advice of Charge (Charging) (AoCC)

Definition

This service provides the means by which the mobile station (MS) may indicate the charge that will be made for the use of telecommunication services. It is intended for applications where the user is generally not the subscriber but is known to the subscriber, and where the user pays the subscriber, rather than the Service Provider.

The charge information is based as closely as possible on the charge that will be levied on the subscriber's bill in the Home PLMN. Where this charge cannot be stored in the MS, use of the telecommunications service shall be prevented as described below [2].

Description

This supplementary service provides the MS with the information to produce an estimate of the cost of the service used. Charges are indicated for the call(s) in progress when mobile originated, or for the roaming leg only, when mobile terminated. Any charges for non-call related transactions, and for certain supplementary services such as Call Forwarding are not indicated.

The MS receives at the beginning of each call (and as necessary during the call) a message, the Charge Advice Information. This message contains the elements, which together define the rate at which the call is to be charged, time dependence, data dependence and for unit increments.

The MS still indicates appropriate charges, even when roaming, based on Home PLMN units.

Where applicable, the volume charge for Packet data service is indicated in addition to the normal time dependent and incremental charges.

To indicate the charge per call, the mobile station displays the units consumed so far during the present call(s) and maintains this value until the MS is switched off or a new call setup is attempted.

Where required to indicate the total accumulated charge, the MS displays, and the SIM stores in the ACM the running cumulative unit charge.

This value must be stored securely and all reasonable steps must be taken to ensure that the written value cannot be interrupted, reset, or corrupted (except resetting under control of the unblocking key).

Barring of incoming calls (BAIC, BAIC-Roam)

Definition

This service makes it possible for a mobile subscriber to have barring of certain categories of incoming calls according to a barring program which is selected from a set of one or more barring programs chosen at provision time and is valid for all incoming calls, or just those associated with a specific basic service group [3].

The ability of the served mobile subscriber to set-up outgoing calls remains unaffected.

Description

The mobile subscriber may determine by subscription of a set of one or more barring programs what kind of incoming calls shall be barred.

The following barring programs are defined:

- Barring of all incoming calls;
- Barring of incoming calls when roaming outside the home PLMN country.

The PLMN will ensure that only one of the barring programs is active per basic service group. The activation of one specific barring program will override an already active one (i.e. the old one will be permanently deactivated).

Description of contents of barring programs:

- Barring of all incoming calls.

  With this barring program there will be no set-up of incoming calls to the served subscriber.

- Barring of incoming calls when roaming outside the home PLMN country.

  With this barring program, calls which are terminated for the served subscriber will be barred if the subscriber is roaming outside the home PLMN country (i.e. the program is active and operative). The ability to receive calls in the home PLMN country remains unaffected (i.e. the program is active and quiescent).

Barring of outgoing calls (BAOC, BOIC, BOIC-exHC)

Definition

This service makes it possible for a mobile subscriber to have barring of certain categories of outgoing calls according to a barring program which is selected from a set of one or more barring programs chosen at provision time and is valid for all outgoing calls, or just those associated with a specific basic service group. The ability of the served mobile subscriber to receive calls and to set-up emergency calls remains unaffected [3].

Description

The mobile subscriber may determine by subscription of a set of one or more unique barring programs what kind of outgoing calls shall be barred.

The following barring programs are defined:

- Barring of all outgoing calls.
- Barring of outgoing international calls.

The PLMN will ensure that only one of the barring programs is active per basic service group. The activation of one specific barring program will override an already active one (i.e. the old one will be permanently deactivated).

Description of contents of barring programs:

- **Barring of all outgoing calls.**

  With this barring program there are no outgoing set-up possibilities, except emergency calls.

- **Barring of outgoing international calls.**

  Outgoing call set-up possibilities exist only to subscribers of the PLMN(s) and the fixed network(s) of the country where the mobile subscriber is presently located. So the present PLMN may be the home PLMN or a visited PLMN, respectively the fixed network may be that of the home PLMN country or that of a visited PLMN country.

- **Barring of all outgoing international calls except those directed to the home PLMN country.**

  Outgoing call set-up possibilities exist only to subscribers of the PLMN(s) and the fixed network(s) of the country where the mobile subscriber is presently located or to mobile subscribers of the home PLMN country of the served mobile subscriber and to subscribers of the fixed network(s) in the home PLMN country. So the present PLMN may be the home PLMN or a visited PLMN, respectively the fixed network may be that of the home PLMN country or that of a visited PLMN country.

Call Forwarding Unconditional (CFU)

Definition

This service permits a called mobile subscriber to have the network send all incoming calls, or just those associated with a specific Basic service group, addressed to the called mobile subscriber's directory number to another directory number. The ability of the served mobile subscriber to originate calls is unaffected. If this service is activated, calls are forwarded no matter what the condition of the termination [4].

Description

The served mobile subscriber can request a different forwarded-to number for each Basic service group containing a basic service to which they have subscribed.

Call Forwarding on Mobile Subscriber Busy(CFB)

Definition

This service permits a called mobile subscriber to have the network send all incoming calls, or just those associated with a specific Basic service group, addressed to the called mobile subscriber's directory number and which meet mobile subscriber busy to another directory number. The ability of the served mobile subscriber to originate calls is unaffected. If this service is activated, a call is forwarded only if the call meets mobile subscriber busy [4].

Description

The served mobile subscriber can request a different forwarded-to number for each Basic service group containing a basic service to which they have subscribed.

Call Forwarding on Mobile Subscriber Not Reachable (CFNRc)

Definition

This service permits a called mobile subscriber to have the network send all incoming calls, or just those associated with a specific Basic service group, addressed to the called mobile subscriber's directory number, but which is not reachable, to another directory number.

The ability of the served mobile subscriber to originate calls is principally unaffected, but practically it is affected if the mobile subscriber is de-registered, if there is radio congestion or if the mobile subscriber for example is being out of radio coverage. If this service is activated, a call is forwarded only if the mobile subscriber is not reachable [4].

Description

The served mobile subscriber can request a different forwarded-to number for each Basic service group containing a basic service to which he has subscribed.

Call Forwarding on No Reply (CFNRy)

Definition

This service permits a called mobile subscriber to have the network send all incoming calls, or just those associated with a specific Basic service group, addressed to the called mobile subscriber's directory number and which meet no reply to another directory number. The ability of the served mobile subscriber to originate calls is unaffected. If this service is activated, a call is forwarded only if the call meets no reply [4].

Description

The served mobile subscriber can request a different forwarded-to number for each Basic service group containing a basic service to which they have subscribed.

Call Hold (HOLD)

Definition

The call hold service allows a served mobile subscriber, who is provisioned with this Supplementary Service, to interrupt communication on an existing active call and then subsequently, if desired, re-establish communication. The traffic channel remains assigned to the mobile subscriber after the communication is interrupted to allow the origination or possible termination of other calls [5].

Description

When the call hold service is invoked, communication is interrupted on the traffic channel and the traffic channel is released from the existing call. The traffic channel is reserved for the served mobile subscriber invoking the call hold service. The served mobile subscriber can only have one call on hold at a time.

One traffic channel should be reserved for the served mobile subscriber as long as the subscriber has one call on hold and is currently not connected to any other call, i.e. the network should not reserve more than one traffic channel for a mobile station.

If the served mobile subscriber has a call on hold and is not connected to an active call, she can:

- Retrieve the held call.
- Set up another call.
- Disconnect the held call.

If the served mobile subscriber has a call on hold and is not connected to an active call she cannot receive a call, except when using the Call Waiting Supplementary Service.

If the served mobile subscriber is connected to an active call and has another call on hold, she can:

- Alternate from one call to the other.
- Disconnect the active call.
- Disconnect the held call.
- Disconnect both calls.

If the served mobile subscriber is connected to an active call and has another call on hold, they cannot receive a call.

Call Waiting (CW)

Definition

The Call Waiting Service permits a mobile subscriber to be notified of an incoming call whilst the traffic channel is not available for the incoming call and the mobile subscriber is engaged in an active or held call. Subsequently, the subscriber can either accept, reject, or ignore the incoming call [5].

Description

This service operates when the traffic channel at the controlling subscriber B is not available and B is engaged in an active or held call.

When a third party attempts to connect to that termination, the controlling subscriber B is given an appropriate indication of the waiting call. A notification that the call is waiting will be sent back towards the calling subscriber C.

The maximum number of waiting calls at one time per mobile access is one. This means that no further calls are offered to the subscriber while a call is waiting.

Calling Line Identification Presentation (CLIP)

Definition

The CLIP Supplementary Service provides the called party with the possibility to receive the line identity of the calling party [6].

Description

This Supplementary Service provides for the ability to indicate the line identity of the calling party to the called party.

The network shall deliver the calling line identity to the called party at call set-up time, regardless of the terminal capability to handle the information.

Calling Line Identification Restriction (CLIR)

Definition

The CLIR Supplementary Service enables the calling party to prevent presentation of its line identity to the called party [6].

Description

The CLIR Supplementary Service is a Supplementary Service offered to the calling party to prevent presentation of the calling party's line identity, to the called party.

Connected Line Identification Presentation (COLP)

Definition

The Connected Line Identification Presentation (COLP) Supplementary Service provides the calling party with the possibility to receive the line identity of the connected party [6].

Description

This Supplementary Service is not a dialing check but an indication to the calling subscriber of the connected line identity in a full ISDN/GSM environment, the connected line identity shall include all the information necessary to unambiguously identify the connected party.

The network shall deliver the connected line identity to the calling party regardless of the terminal capability to handle the information.

Connected Line Identification Restriction (COLR)

Definition

The COLR Supplementary Service enables the connected party to prevent presentation of its line identity to the calling party [6].

Description

The COLR Supplementary Service is a Supplementary Service offered to the connected party to prevent presentation of the connected line identity, to the calling party.

Multi-Party Service (MPTY)

Definition

This Supplementary Service provides a mobile subscriber with the ability to have a multi-connection call, i.e. a simultaneous communication with more than one party [7].

Description

A precondition for the multi-party service is that the served mobile subscriber is in control of one active call and one call on hold, both calls having been answered. In this situation the served mobile subscriber can request the network to begin the MultiParty service.

Once a MultiParty call is active, remote parties may be added, disconnected or separated (i.e. removed from the MultiParty call but remain connected to the served mobile subscriber).

Closed User Group (CUG)

Definition

The Closed User Group (CUG) Supplementary Service enables subscribers, connected to a PLMN and possibly also other networks, to form closed user groups (CUGs) to and from which access is restricted.

A specific user may be a member of one or more CUGs. Members of a specific CUG can communicate among each other but not, in general, with users outside the group. The ability to set up emergency calls remains unaffected [8].

Description

An ISDN/MSISDN number shall identify each member of a CUG.

A CUG shall be defined for one or more basic service groups.

CUG members can have additional capabilities that allow them to originate calls outside the group, and/or to receive calls from outside the group. CUG members can have additional restrictions that prevent them from originating calls to other members of the CUG, or from receiving calls from other members of the CUG.

CUG shall remain unaffected when members roam to PLMNs supporting CUG. Roaming subscribers must have the same CUG facilities on the roamed-to PLMN as on the Home PLMN.

When roaming to networks not supporting CUG, the CUG restrictions must be enforced.

Each individual subscriber may be a member of a maximum of 10 CUGs.

Explicit Call Transfer (ECT)

Description

Explicit call transfer allows a user (user A) with two calls (one active-user B and the other on hold-user C) to be combined together on one call. Each call can be either an incoming call or outgoing call. ECT permits user A to connect User B & C together into one call and allow user A to disconnect from the call [9].

Enhanced Multi-Level Priority & Precedence (EMLPP)

The Tekelec ngHLR supports the EMLPP feature to provide Wireless Priority Service (ex: priority of 911 calls over other calls, over the entire network).

This feature is implemented as a service that the operator can or cannot use optionally to a domain of his network. The domain can be the whole network or a subset of the network. The EMLPP service applies to all network resources in the domain that is in common use.

This service has two parts - precedence and pre-emption. Precedence involves assigning a priority level to a call in combination with fast call set-up. Pre-emption involves the seizing of resources, which are in use by a call of a lower precedence, by a higher level precedence call in the absence of idle resources. Pre-emption can also involve the disconnection of an on-going call of lower precedence to accept an incoming call of higher precedence.

The EMLPP service is applicable to all mobile stations in the domain with all or some mobile stations having a respective subscription assigning precedence according to the EMLPP service. The EMLPP

is a supplementary service and shall be provided to a subscriber for all basic services subscribed to and for which EMLPP applies.

The EMLPP information is stored in the HLR. If included in the Insert Subscriber Data request, this parameter defines the priorities the subscriber might apply for a call.

If the VLR does not support the EMLPP service it returns its code to the HLR in the parameter SS-Code List and therefore discards the received information (no error is sent back).

The EMLPP subscription data that have been stored previously in a subscriber data record in the VLR are completely replaced by the new EMLPP subscription data received in a `MAP_INSERT_SUBSCRIBER_DATA` during either an Update Location or Restore Data procedure or a standalone Insert Subscriber data procedure. This parameter is used only by the VLR and if the SGSN receives this parameter it shall ignore it.

To provision this service, a new table has been added in the Subscriber Profile entity. Please refer to the "Enhanced Multi-Level Priority & Precedence (EMLPP)" section in the *SDM Subscriber Provisioning - Reference Manual* for more information on the EMLPP parameters. For step-by-step instructions on how to provision the EMLPP service from the WebCI, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Validation of subscriber data provisioning for Supplementary Services and Forward-To-Numbers

The HLR Provisioning process has the capability to perform a validation of the subscriber data provisioned with respect to the Supplementary Services (SS) and Forward-To-Number (FTN) from the OAM interface. The validation performed from the OAM interface is as per the 3GPP standards and the same as the validation of the traffic interface. In other words, the Tekelec ngHLR is capable of performing a FTN validation and SS interactions validation as per the 3GPP standards.

While the SS data is always validated through both the OAM and traffic interface, the FTN data is always validated through the traffic interface, but not through the OAM interface. By default, the FTN validation is not performed through the OAM interface.

The Network Operator can activate/deactivate the validation of FTNs provisioned through the OAM interface on a global basis and on a per subscriber basis. To achieve this, the following two parameters have been implemented:

- The HlrConfig entity's 'FtnProvValidation' parameter allows the Network Operator to activate/deactivate globally (system-wide) the validations of provisioned FTNs through the OAM interface. By default, the FTN validation is deactivated.
- The 'FtnOverride' parameter of the Subscriber Profile's CallForwardBsg[] entity allows to bypass the validation of the provisioned FTNs through the OAM interface on a per subscriber basis when the global FTN validation is activated ('FtnProvValidation' = '1'). Take note that the value of this flag is not permanent and must be specified for each transaction.

Whenever the validation of a provisioning request fails, the ngHLR rejects it and returns an error notification in order to provide more guidance and information about the problem. Refer to the "Error Notifications" section of the *SDM Monitoring, Maintaining, Troubleshooting-Reference Manual* for details on the error notifications.

For details on the 'FtnProvValidation' parameter, refer to the "HLR Configuration" section of the *SDM System Configuration - Reference Manual*. For details on the 'FtnOverride' parameter, refer to the "Call Forward - Basic Service Group" section of the *SDM Subscriber Provisioning - Reference Manual*. For instructions on how to provision the HLR Configuration data from the WebCI, refer to the "Configuring the HLR" section of the *SDM System Configuration - User Guide*. For instructions on how to provision

Call Forward - Basic Service Groups from the WebCI, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

For any other instructions on how to provision subscribers and supplementary services using XML requests, refer to both the *SDM Subscriber Provisioning-Reference Manual* and the *SDM Subscriber Provisioning-User Guide*.

Operator Determined Barring

Application of Operator Determined Barring is controlled by the Service Provider, by administrative interaction with the HLR; this interface is not standardized.

With the exception of the barring of roaming, the HLR effects Operator Determined Barring in a similar manner to Service Provider - activated use of the Call Barring Supplementary service. Consequently, the VLR and MSC also execute the relevant Barring Conditions in similar manners. It is noted that there is no password usage. Roaming is barred by the HLR when the MS is in a PLMN other than the Home PLMN or not in the Home PLMN Country as applicable.

In addition to ensuring the barring integrity for future calls, the HLR, and consequently the MSC and VLR, shall provide means to terminate the calls of a user that have been established prior to the application of the ODB service and which are still ongoing [10].

GPRS

The GPRS allows the service subscriber to send and receive data in an end-to-end packet transfer mode, without utilizing network resources in circuit switched mode [11].

GPRS enables the cost effective and efficient use of network resources for packet mode data applications e.g. for applications that exhibit one or more of the following characteristics:

- intermittent, non-periodic (i.e., bursty) data transmissions, where the time between successive transmissions greatly exceeds the average transfer delay
- frequent transmissions of small volumes of data, for example transactions consisting of less than 500 octets of data occurring at a rate of up to several transactions per minute
- infrequent transmission of larger volumes of data, for example transactions consisting of several kilobytes of data occurring at a rate of up to several transactions per hour

Within the GPRS, two different bearer service types are defined. These are:

- Point-To-Point (PTP)
- Point-To-Multipoint (PTM)

Based on standardized network protocols supported by the GPRS bearer services, a GPRS network administration may offer (or support) a set of additional services.

Some examples of teleservices which may be supported by a PTM bearer service include:

- Distribution services
    - Which are characterized by the unidirectional flow of information from a given point in the network to other (multiple) locations. Examples may include news, weather and traffic reports, as well as product or service advertisements
- Dispatching services

  - Which are characterized by the bi-directional flow of information from a given point in the network (dispatcher) and other (multiple) users. Examples include taxi and public utility fleet services

- Conferencing services
  - Which provide multi-directional communication by means of real-time (no store-and-forward) information transfer between multiple users

Capabilities that may be offered together with the PTM bearer services include:

- Geographical routing capability
  - Which provides the ability to restrict message distribution to a specified geographical area
- Scheduled delivery capability
  - Allowing store-and-forward type services to specify a future delivery time and a repetition rate

It is possible to include these capabilities as part of the service request (i.e., as part of the packet). Some operators may offer PTM services only together with these capabilities.

EGPRS is an enhancement of GPRS allowing higher data rates on the radio interface. The same set of services provided by GPRS is available in EGPRS.

Tekelec ngHLR GPRS enhancement feature supports "Network-Requested PDP Context Activation services". This feature is used by the GGSN (Gateway GPRS Support Node) to interrogate the MS (Mobile Station) routing information from the HLR and is used by an HLR to update the MS's PDP context status from the GGSN.

It supports the following services:

- MAP_SEND_ROUTING_INFO_FOR_GPRS. The GGSN requests GPRS routing information from the HLR
- MAP_FAILURE_REPORT. The GGSN informs the HLR that the network requested PDP-context activation has failed.
- MAP_NOTE_MS_PRESENT_FOR_GPRS. The HLR informs the GGSN that the MS is present for GPRS again.

Support for Extended Uplink QoS bit rate and HSPA+

The Tekelec ngHLR supports an extended uplink and downlink quality of service (QoS) bit rate of up to 256 Mbps.

HSPA+ is Evolved High-Speed Packet Access. It is a technical standard for wireless and broadband telecommunications. HSPA+ enhances 3G networks with higher speeds for the end user and is comparable to the newer LTE networks.

Both these are detailed in the *3GPP TS 24.008 V8.13.0 (2011-03)* technical specification.

This section identifies affected provisioning components for this feature and the location of additional information.

Table 15: Provisioning Information

Affected Components	Description	Reference
Interfaces	CLI, WebCI	
Main Tables[]/attributes	To provision the uplink and downlink quality of service (QoS) bit rate, set the following optional attributes in the GPRS Context table: • QosMaxBitRateUp • QosMaxBitRateDown • QosGuaranteedBitRateUp • QosGuaranteedBitRateDown	*SDM Subscriber Provisioning Reference Manual* • Home Location Register (HLR) • GPRS Services
Alarms	None	---
Error Messages	None	---
Counters	None	---
Procedures	Provisioning a subscriber HLR service profile: Viewing/editing subscriber profiles	*SDM Monitoring, Maintaining, Troubleshooting User Guide*

Note: The QosPeakThroughput is the binary representation of the peak throughput class. If the Network Operator changes the values of the QosMaxBitRateUp, QosMaxBitRateDown, QosGuaranteedBitRateUp or QosGuaranteedBitRateDown then the value of the QosPeakThroughput is generated by the ngHLR using rules specified in the 3GPP standard.

Super-charged HLR

Super-Charger is a network feature which reduces mobility management costs associated with inter-VLR and SGSN location updates by reducing signaling.

In Super-Charged networks, whenever a subscriber moves to a location area served by a different MSC/VLR, its subscription data are retained in the old MSC/VLR. Consequently, the HLR does not need to perform the cancel location procedure at the old MSC/VLR. Whenever the subscriber roams to a previously visited network, provided that the retained subscription data are still valid, the HLR does not need to perform the insert subscriber data procedure at the MSC/VLR. Super-Charger is equally applicable to packet services.

Super-Charger is of most benefit in metropolitan areas having a high density of MSC/VLRs to cope with a large number of subscribers and where subscribers regularly commute between different location areas.

Short message service management

Mobile terminated short message transfer procedure

The mobile terminated short message transfer procedure is used to transfer (or forward) a short message or several short messages from a Short Message Service Centre to a mobile subscriber [1].

Short message alert procedure

The Short Message Alert procedure is used to alert the Short Message Service Centre when the mobile subscriber is active after a short message transfer has failed because the mobile subscriber is not reachable or when the MS has indicated that it has memory capacity to accept a short message.

Short message delivery status report procedure

The SM delivery status report procedure is used to set the Short Message Service Centre address into the message waiting list in the HLR because the subscriber is absent or unidentified or the memory capacity is exceeded.

The procedure sets

- the memory capacity exceeded flag in the HLR if the MS memory does not have room for more messages
- and/or the MS not reachable flag for non GPRS in the case of unidentified or absent subscriber
- and/or the MS not reachable for GPRS flag in the case of unidentified or absent subscriber for GPRS

CAMEL Phase 2

The CAMEL network feature enables the use of Operator Specific Services (OSS) by a subscriber even when roaming outside the HPLMN [12].

- Any time interrogation - If an OSS needs the Subscriber State and/or the Location Information, the gsmSCF initiates a transaction to the HLR by sending an Any_Time_Interrogation Request. Support for this procedure is a network operator option.
- Delete subscriber data - This service is used by an HLR to remove certain subscriber data from a VLR if the subscription of one or more supplementary services or basic services is withdrawn.

  Note: This service is not used in case of erasure or deactivation of supplementary services.

- Insert subscriber date - This service is used by an HLR to update a VLR with certain subscriber data in the following occasions:

  - the operator has changed the subscription of one or more supplementary services, basic services or data of a subscriber.

    Note: In case of withdrawal of a Basic or Supplementary service this primitive shall not be used.

  - the operator has applied, changed or removed Operator Determined Barring
  - the subscriber has changed data concerning one or more supplementary services by using a subscriber procedure
  - the HLR provides the VLR with subscriber parameters at location updating of a subscriber or at restoration. In this case, this service is used to indicate explicitly that a supplementary service is not provisioned, if the supplementary service specification requires it. The only supplementary services which have this requirement are the CLIR and COLR services. Network access mode is provided only in restoration. If the Super-Charger functionality is supported the HLR may not need to provide the VLR with subscriber parameters at location updating of a subscriber. See TS 24.116

Also this service is used by an HLR to update an SGSN with certain subscriber data in the following occasions:

- if the GPRS subscription has changed
- if the network access mode is changed
- the operator has applied, changed or removed Operator Determined Barring
- the subscriber has changed data concerning one or more supplementary services by using a subscriber procedure
- the HLR provides the SGSN with subscriber parameters at GPRS location updating of a subscriber. If the Super-Charger functionality is supported the HLR may not need to provide the SGSN with subscriber parameters. See 3G TS 24.116

It is a confirmed service and consists of the primitives shown in table 8.8/1.

This IF is specified in GSM 09.02 [4] and used by the HLR to insert subscriber data in the VLR.

- Provide subscriber info
  - This service is used by the HLR to request information (subscriber state and location) from the VLR at any time.
- Provide roaming number
  - This is used by the HLR to request a roaming number from the VLR.
- Update location
  - This is used by the VLR to provide the information about supported CAMEL phases to the HLR

When requesting location updating or data restoration the VLR shall indicate to the HLR which CAMEL phases it supports.

The CAMEL phase 2 HLR shall then send to the VLR CAMEL subscription data for one of the CAMEL phases supported by the VLR or, if some different handling is required, data for substitute handling.

- Restore Data
  - This is used by the VLR to provide the information about supported CAMEL phases to the HLR
- Send routing info
  - This is used by the HLR when the GMSC requests information from the HLR to route a call. The HLR will send back a reply containing information such as subscriber location, subscriber state, originating and terminating CAMEL services, basic service code, and CUG subscription information.

CAMEL Phase 3

Support for CAMEL Phase 3 on the Tekelec ngHLR intends to augment the existing CAMEL Phase 1 and CAMEL Phase 2 support with more (CSIs) CAMEL Subscription Indicators (D-CSI, GPRS-CSI, M-CSI, OSMS-CSI, VT-CSI), along with the associated logic, and additional Trigger Detection Points (TDPs) for O-CSI and T-CSI.

CAMEL Phase 1 and 2 included support for:

- CAMEL Subscription Information: O-CSI, T-CSI, SS-CSI, Tif-CSI, U-CSI, UG-CSI
- Support for Any Time Interrogation (ATI)
- Support for CAMEL TDP Criteria at HLR

CAMEL Phase 3 introduces the following additional CSIs:

- D-CSI support: The D-CSI is transferred from Tekelec ngHLR to MSC at Location Update and to GMSC during termination call handling. Based on the presence of D-CSI a subscribed dialed service may be invoked during a MO or MT Call establishment at DP AnalyzedInfo. The dialed service is invoked/or not based on the trigger information contained in the D-CSI.
- GPRS-CSI support: The GPRS-CSI is transferred from ngHLR to SGSN at Location Update. The GPRS-CSI allows the invocation of subscribed CAMEL services at the SGSN. GPRS-CSI may contain trigger information related to the GPRS state model (TDP "Attach", or "AttachChangeOfPosition") or related to the GPRS PDP Context state Model (TDP "PdpContextEstablishment", PdpContextEstablishmentAck", "ChangeOfPosition") . Depending on the content of the GPRS-CSI, Camel Service may be invoked at any of the armed TDPs above.
- M-CSI support: The M-CSI is transferred from Tekelec ngHLR to MSC at Location Update M-CSI allows triggering of notifications from MSC to gsmScf based on a specific mobility event (Location Update in VLR, Location Update to other VLR, MS-initiated IMSI detach, IMSI attach, Network Initiated IIMSI detach). Those notifications may be used to keep track of the state and location of the subscriber (needed for the implementation in some IN services), etc.
- OSMS-CSI support: The OSMS-CSI is transferred from Tekelec ngHLR to MSC/SGSN at Location Update. The OSMS-CSI allows the MSC/SGSN to invoke a Camel Service in the gsmScf at the submission of SMS by the subscriber.
- VT-CSI (VMSC Terminating CSI) support: The VT-CSI is transferred from Tekelec ngHLR to MSC at Location Update. The VT-CSI allows Camel Service to be invoked when termination call arrives at the VMSC. The VMSC contacts the VLR and if the subscriber has VT-CSI, the MSC invokes a Camel Service if the triggering criteria contained in the VT-CSI are fulfilled.

CAMEL Phase 3 introduces the following Trigger Detection Points (TDPs):

Route_Select_Failure:TDP Route_Selct_Failure applies to O-CSI fro MO calls and to MF calls (in GMSC and VMSC)

- T_busy and T_No_Answer: TDPs T_busy and No_Answer apply to T-CSI for MT calls and to VT-CSI for VT calls. Those TDPs may have trigger criteria associated with them. The trigger criteria (defined per TDP) consists of a list of up to 5 ISUP cause values. When trigger criteria are present, triggering of a Camel service invocation will take place only when the cause value of the failure matches any of the cause values in the triggering criteria.
- The Tekelec ngHLR now provides Active Location retrieval as an enhancement of ATI. With ALR the gsmScf may instruct the VLR to page the subscriber. The ALR is triggered and implemented using the parameters "current location" in ATI, PSI and "current location retrieved" in the location information of the PSI-Res

With the support of new CSIs and new functionalities for Camel Phase 3, new provisioning entities have been implemented. Refer to the "Camel services" section of the *SDM Subscriber Provisioning - Reference Manual* for more details on the new entities and parameters that need to be provisioned for a CAMEL subscriber and refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*, to know how to provision a subscriber with CAMEL services from the WebCI.

HLR USSD Handling

Unstructured Supplementary Service Data (USSD) is a mechanism in GSM networks that provides session-based messaging between mobile station users and operator defined mobile applications. It transmits text information over the signaling channels of a GSM network.

Thus, the mobile station user and the application communicate in a manner that is transparent to the MS and to intermediate network entities.

USSD benefits:

- USSD provides an ideal mechanism for the mobile terminal to access mobile services such as callback when roaming. Because messages can be exchanged with the HLR, subscribers can send USSD messages back to the network even when they are roaming on other networks. Thus home network services continue to work just as well even when subscribers are roaming.
- Turnaround response times for interactive applications are shorter for USSD than compared to SMS times.
- Mobile users can enter USSD commands directly from their initial mobile phone screen. They do not need to access any particular phone menu. Commands are dialed in the format *123#, where 123 is a defined number serving a specific service.
- The commands are routed back to the home mobile network's Home Location Register (HLR). The HLR then routes the USSD message to the appropriate mobile application for processing.

USSD sessions can be initiated by the Mobile user or by the network. The SDM currently supports USSD messages in English, the GSM 7 bit alphabet, and messages encoded with "unspecified language".

A USSD Allowed Flag has been implemented to allow the operator to enable/disable the processing of USSD messages for a specific subscriber. This flag can be provisioned on a per subscriber basis and the Tekelec ngHLR behaves as follows:

- In the case where the USSD-Allowed Flag is enabled, the Tekelec ngHLR routes the USSD messages to the appropriate mobile application for processing.
- When a Mobile Subscriber initiates a USSD message and in the case where the USSD-Allowed Flag is disabled in its subscriber profile, the Tekelec ngHLR returns a `MAP_U_ERROR` message with the "callBarred" error.
- When the Network operator initiates a USSD message for a subscriber for which the USSD-Allowed Flag is disabled, the Tekelec ngHLR returns a `MAP_U_ERROR` message with the "`illegalSubscriber`" error.

Active Location Retrieval

This feature allows the gsmSCF to retrieve the latest location of a subscriber, as stored in the VLR during the most recent location update procedure.

Active Location Retrieval (also known as current location retrieval) is an enhancement to MAP Any Time Interrogations (ATI) messages. With MAP ATI messages, the gsmSCF may obtain the subscriber's location information as currently stored in the VLR. The information in the VLR is stored during the most recent update location procedure. The location update procedure may be due to the subscriber changing location to another location area, call establishment or periodic location update.

With the ALR feature, the gsmSCF may instruct the VLR to page the subscriber, in which case the location information in the VLR will be refreshed and will then include the current cell id of the subscriber.

The following parameters, used to characterize the location of the subscriber, are supported in the MAP operations by the Tekelec ngHLR:

- Age of location
- Geographical Information
- VLR Number

- Location Number

The Tekelec ngHLR simply takes on the role of extracting the information from the ATI message received from the gsmSCF, and encapsulating it into a PSI message, destined to the VLR. The same mechanism is used for the PSI_response to the ATI

The ATI message contains a field (Current Location) that must be set to 1 in order to request a subscriber's active location. In the response message, the location information (Age of location, Geographical Information, VLR Number, Location Number) will be present or not, depending on the value of that field.

When an ALR is requested while the subscriber is in radio contact with the MSC/VLR (e.g. during a call), the MSC will not perform paging. However, the stored location in VLR is in that case already the current location. If the subscriber is detached from the MSC, then no paging will take place either.

This enhancement of the location update process is syntactically backwards compatible. The MAP operation versions used for the active location retrieval procedure are the same as for the regular location retrieval procedure. If the VLR does not support the transport of these parameters in the respective MAP operations, then the MAP respective operations are processed as for regular location retrieval procedure. That implies that the location retrieval succeeds, but without paging. The gsmSCF obtains the information stored in the VLR, but deduces from the absence of "*current location retrieved*" that the subscriber was not paged.

MAP Version negotiation

The Tekelec ngHLR supports the MAP Version Compatibility feature. This feature ensures that network entities supporting different MAP release versions are still able to provide service to the subscriber. It supports complete backward compatibility with network entities at MAP version 2. It will also negotiate acceptable Application Context (AC) versions when interacting with an unknown network entity. The latest AC version supported by the HLR is given in GSM MAP Release 4 specification (3GPP 29.002 v4.11.0).

UMTS Support

This feature allows the Tekelec ngHLR to be deployed in a UMTS (3G) network and to offer UMTS services to the subscribers.

More precisely, the UMTS feature has been implemented in order to enable the Tekelec ngHLR to:

- Support UMTS subscriber profiles and their USIM card.
- Provide UMTS subscribers with security by supporting UMTS Authentication procedures and algorithms by including UMTS Milenage and UMTS XOR.
- Support the necessary MAP version negotiation and authentication quintuplet/triplet conversion to allow UMTS subscribers roaming in GSM networks (R98 VLRs and earlier).
- Support UMTS (R99+), HSDPA (R5) and HSUPA (R6) data models by extending the QoS fields of the Tekelec ngHLR subscriber profile.

Subscriber Categories

This feature enables the support of provisioning and managing different Subscriber Categories in the Tekelec ngHLR subscriber profiles, and sending the Subscriber Category in the ISD messages. This feature allows the operator to provision new custom services. The use of Subscriber Categories in the 3GPP subscriber profile is referenced in TS23.008, and the list of possible categories is defined in ISUP specification ITU-T Q.763.

With this feature:

- The Tekelec ngHLR supports all subscriber categories defined in ITU-T Q.763.
- The subscriber's category used by the Tekelec ngHLR by default is CAT10= Ordinary calling subscriber.
- The Tekelec ngHLR sends the subscriber category in the ISD message after a successful Update Location.
- The operator can provision one subscriber category indicator per subscriber profile (Primary IMSI) when provisioning through all interfaces (WebCI, CLI, SOAP/XML interface, XML bulk subscriber provisioning and provisioning using templates).
- The Tekelec ngHLR sends a standalone ISD message when the subscriber category of a subscriber is modified through a provisioning interface.

For more information on the **Subscriber Category** field (MsCat) and its possible values, please refer to the "Subscriber Profile (Bearer Services, TeleServices, Call Barring, PreferredRoutingNetworkDomain)" section of the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision the Subscriber Category field (MsCat) from the WebCI, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

GSM Bearer Capabilities

The first phase of the GSM Bearer Capabilities feature has been implemented in the Tekelec ngHLR. This enables the Tekelec ngHLR to communicate bearer capabilities information to the VLR through the Provide Roaming Number message. With the implementation of this feature, a new GsmBearerCapabilities (BC) entity has been created to allow the operator to define Bearer Capabilities and new fields have been added to the subscriber's profile to be able to associate a BC to each of the subscriber's MSISDN.

The first phase of the implementation of the BC feature is as per the "Multiple Numbering Scheme" in section 9.2.2 of the 3GPP TS 29.007 v 4.12.0. Functionalities like voice, fax, data, etc. are distinguished by using a different MSISDN.

When the Tekelec ngHLR receives an interrogation relating to an incoming call (i.e. the MAP "Send Routing Information" procedure), it requests a roaming number (MSRN) from the VLR. This request will contain the PLMN BC reflecting the service associated with the called MSISDN. The PLMN BC is passed to the VLR within the MAP parameter "GSM Bearer Capability" of the message "Provide Roaming Number".

The GSM Bearer Capabilities feature can be provisioned through the CLI and WebCI, as follows:

- By provisioning the GsmBearerCapabilities [ ] table with different BC information and identifying each of them with a different Bearer Capability Name.
- By provisioning the GsmBearerCapabilitiesB3x [ ] table, if necessary. This allows to provision BC information occupying the octets B3b, B3c, B3d, etc. Refer to the 3GPP standard TS 24.008 for more detailed octet information in a Bearer Capability element.
- By associating BC information, defined in the GsmBearerCapabilities [ ] table, to each MSISDN for which you wish the Tekelec ngHLR to send BC information. The Tekelec ngHLR sends the Provide Roaming Number message with the correct BC information if it is associated to its MSISDN. If no BC information is associated to the subscriber's MSISDN, the Tekelec ngHLR won't send any BC information in the PRN message.

For more information on the Bearer Capabilities tables and their fields and possible values, please refer to the *"GSM Bearer Capabilities"* and "MSISDN" sections of the *SDM System Configuration - Reference*

Manual. For step-by-step instructions on how to provision the Gsm Bearer Capabilities tables and on how to associate them to a MSISDN, please refer to the "Provisioning GSM Bearer Capabilities" section of the *SDM System Configuration - User Guide* and to the MSISDN table in the "Viewing/Editing SIM cards, MSISDNs, IMSIs and HLR Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Addition of GSM Bearer Capabilities and Bearer Services in SRI-ack

The GSM Bearer Capabilities feature has been enhanced by adding the option to return the GSM Bearer Capabilities and Bearer Services information in the SRI-ack response to the GMSC. This option can only be used for messages using the MAP version 7 and up.

A flag has been implemented in the HLR's database in order to allow the default behavior to be disabled in the case where the GSM-BC and BS information must be excluded in the SRI-ack message. The operator can provision this BcInSriAck flag in the Map Policing's AcTemplate entity from the CLI or WebCI. For more details on this new flag and its values, refer to the "MAP Policing" section of the *SDM System Configuration-Reference Manual*.

With the implementation of this feature, the Tekelec ngHLR now includes for all the subscribers the GSM-BC and BS information in the SRI-ack response in the following conditions:

- The BcInSriAck flag is set to the default value (`'1'`), which indicates that the GSM-BC and BS data must be included in the SRI-ack message.
- The T-CSI Suppression is disabled (Inhibition flag in the CamelCsiData entity is set to (`'0'`).
- The MSISDN has an associated PLMN-BC provisioned in the database.

In the case where at least one of these conditions is not met, the Tekelec ngHLR doesn't include the GSM-BC and BS information in the SRI-ack response.

MAP segmentation on SAI-ack

The "MAP segmentation on SAI-acknowledgement" feature has been implemented in order to allow the Tekelec ngHLR to support MAP segmentation on the Send-Authentication-Information acknowledgement (SAI-ack) message. This enables the Tekelec ngHLR to reply to the VLR with a Send-Authentication-Information acknowledgement message that includes more than 4 triplets for a subscriber with a SIM card and with more than 1 quintet for a subscriber with a UMTS SIM card.

This feature can only be configured at installation of the system or by a member of the Tekelec *Customer Care Center*, in which case the HLR must be restarted in order to take effect. It is by default disabled. In the HlrConfig entity, a "SaiAckSegmentation" parameter has been implemented to indicate whether this feature is enabled or disabled. This parameter can be displayed by the operator from the WebCI or CLI.

With this feature enabled, the Tekelec ngHLR performs a segmentation of the SCCP message (UDT) and sends to the VLR the number of SAI-ack messages needed to provide the VLR with the number of authentication vectors requested. The Tekelec ngHLR only performs this under the following conditions:

- the VLR supports MAP Application Context v3
- the VLR requests in the SAI message more than 4 triplets or more than 1 quintet
- the VLR doesn't prohibit segmentation

When the Tekelec ngHLR receives a SAI-Request and these conditions are met, the Tekelec ngHLR answers with a first SAI-ack containing the maximum number of vectors a UDT message can include and leaves the dialog opened. Following this, when the VLR sends back another SAI-request within

the same dialog, the Tekelec ngHLR sends the second SAI-ack with the UDT message containing the remaining number of vectors requested, or the maximum number of vectors possible, depending on the number of vectors initially requested. The Tekelec ngHLR sends to the VLR a series of SAI-ack messages and only closes the dialog when all the number of vectors requested have been provided to the VLR.

This allows the Tekelec ngHLR to send back the exact number of vectors requested in a SAI-Request sent by the VLR.

If this feature is disabled, the Tekelec ngHLR doesn't perform a segmentation of the SCCP message and sends only one SAI-ack message, no matter how many vectors were requested by the VLR's SAI-Request. This means that a maximum of 4 triplets can be sent back in a SAI-ack for a SIM subscriber and a maximum of 1 quintet can be sent back in a SAI-ack for a UMTS SIM subscriber.

For more details on the "SaiAckSegmentation" parameter in the HlrConfig entity, refer to the "HLR Configuration" section in the "HLR entities" chapter of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to display the HlrConfig entity and the "SaiAckSegmentation" parameter, refer to the "Configuring the HLR" section of the *SDM System Configuration - User Guide*.

Default Basic Service Group (DBSG) per MSISIDN

The "DBSG per MSISDN" feature has been implemented to allow the operator to specify a Default BSG for each MSISDN and Alternative MSISDN that needs to be used by the Tekelec ngHLR to handle calls when receiving a SRI message from the GMSC.

With this feature, the operator can provision the following for each MSISDN and Alternative MSISDN from the CLI or WebCI:

- The "BsgOverride" attribute. This attribute represents a flag that indicates whether the Tekelec ngHLR needs to:
  - bypass the analysis of the Network Signaling Information, retrieved from the SRI message, and take the BSG directly from the value provisioned in the Tekelec ngHLR's "DefaultBsg" attribute.
  - analyze the Network Signaling Information retrieved from the SRI message in order to derive a BSG.

- The "DefaultBsg" attribute. The operator can define the default BSG by provisioning the "DefaultBsg" attribute. The Tekelec ngHLR uses this default BSG for basic and supplementary service validation and to invoke SS when handling the SRI request, in either one of these situations:
  - When the SRI message doesn't include the Network Signaling Information.
  - When the SRI message includes the Network Signaling Information and The "BsgOverride" flag is set to On (1=True) or the BSG derivation is not possible.
  - If the "DefaultBsg" attribute is not provisioned, the value used for the default BSG corresponds to SPEECH.

In the case where the SRI message includes the Network Signaling Information and where the "BsgOverride" flag is set to Off (0=False), the Tekelec ngHLR tries to derive the BSG from the Network Signaling Information and uses this derived BSG for basic and supplementary service validation and to invoke SS when handling the SRI request.

The "BsgOverride" and "DefaultBsg" attributes can both be provisioned for a primary MSISDN in the MobileStation entity as well as for each alternative MSISDN in the MultiImsi entity.

For more details on these attributes, refer to the "MSISDN" section of the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision these attributes through the WebCI, refer to the "Viewing/Editing SIM cards, MSISDNs, IMSIs, HLR Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Tekelec ngHLR enhanced features

A4/K4 Transport Encryption Algorithm

This feature enables the support of A4 Transport Encryption Algorithms and K4 Transport keys in the Tekelec AuC provisioning system. This feature has been implemented to increase security by avoiding to send secret information over the internet in clear, such as Ki information. When the Ki is provisioned during the Sim entity provisioning, instead of sending the Ki key in clear, it's rather encrypted with A4/K4 and sent together with an index (i.e., AlgoId), which is used to retrieve the A4/K4 information from the Tekelec ngHLR's database (in the A4K4 entity) in order to decrypt the Ki. The Ki is then encrypted with A7/K7, with which K4 is itself encrypted with, and stored in the database.

A control flag has been implemented to give the operator the possibility to enable or disable the A4/K4 support. By default, this feature is disabled.

In order to use this feature, its control flag along with the A4K4 entity and AlgoId must be provisioned through the WebCI, CLI or using the CmdFileLoader provisioning tool.

This feature works with the following provisioning interfaces: XML/SOAP, CmdFileLoader, Provisioning Templates, TCP Socket and with the CLI and WebCI.

For step-by-step instructions on how to provision this feature through the Blueslice CLI and WebCI, refer to the "Configuring the*A4/K4 Transport Encryption Algorithm"* section in the *SDM System Configuration - User Guide*

. For more detailed information on the parameters used to provision this feature, refer to the "A4/K4 Transport Encryption Algorithm" section in the *SDM System Configuration - Reference Manual* .

Roaming Controls

The Tekelec ngHLR offers to the Network Operator, the capability of controlling some of the Tekelec ngHLR's behavior when a subscriber is roaming. It offers to the Network Operators the ability to customize some features or services on a per roaming PLMN basis.

Currently it consists in giving the operator the ability to:

Define roaming PLMNs as a group of Node ranges, by defining PLMNs with a list of Node ranges (VLR/GMSC address range)

Define Service Screening Templates allowing to Control individual subscriber services like BAOC override mask, Camel Data, etc

Create OCPLMN Templates that contain a list of roaming PLMNs that can be configured individually with different roaming restrictions (list of Allowed IMSI ranges) and service screening restrictions (by referring to a Service Screening Template).

Each subscriber can have a different OCPLMN Template assigned to it, by provisioning the Subscriber Profile with the ID (CLI)/Name (WebCI) of the OCPLMN Template. When receiving an Update Location for a subscriber, the Tekelec ngHLR will use the OCPLMN Template assigned to that subscriber

in order to identify the roaming PLMN and apply the roaming restrictions and service screening restrictions defined for that PLMN.

Operator Controlled PLMN-IMSI selection feature

In GSM/UMTS and GPRS networks, selection of the network (PLMN) is achieved by a combination of algorithms in the SIM card and the terminal and Multi-IMSI implementations are usually based on a Multi-IMSI SIM card. The Operator Controlled PLMN-IMSI selection feature of the Tekelec ngHLR allows a mobile service provider to pre-define a set of allowed PLMN/IMSI combinations.

This feature offers to the mobile service provider a better control on their selection by the SIM/terminal by enabling them to override the SIM card's network selection and IMSI selection process.

The Network Operator can define multiple PLMNs, each with a list of Node Ranges (VLR/GMSC address range). These defined Operator Controlled PLMNs can be assigned to OCPLMN Templates during the latter's creation. This means that an OCPLMN Template can have a list of "allowed" roaming PLMNs, which can each have different roaming restrictions (list of 'allowed' IMSIs for which UL is allowed) and service restrictions assigned to them.

The OCPLMN-IMSI selection feature supports the GSM/UMTS networks by allowing to add VLR address range for a PLMN, as well as the GPRS network by allowing to add GMSC address range for a PLMN.

The Network Operator can dynamically enable/disable the Operator Controlled PLMN-IMSI selection feature through either the CLI or WebCI interfaces, by provisioning the OCPLMN Configuration 'RoamRestrictEnable' parameter. At system start-up, the Roaming Restriction part of the OCPLMN feature is disabled, which means that the Tekelec ngHLR doesn't perform a PLMN-IMSI validation.

If the feature is enabled and the subscriber has an OCPLMN Template assigned to it, upon Location Update, the Tekelec ngHLR executes the PLMN-IMSI validation procedure based on the OCPLMN Template, which consists in validating the following:

that the PLMN is "allowed" (as per configured in the OCPLMN Template).

the PLMN Roaming Restrictions, which consists in validating that the IMSI is "allowed" for the selected PLMN (as per configured in the OCPLMN Template).

If the PLMN-IMSI validation succeeds and in the case where the Roaming Service Screening feature is disabled ('RoamServiceScreeningEnable'=0), then the Tekelec ngHLR processes the Location Update as normally.

If the PLMN-IMSI validation succeeds and in the case where the Roaming Service Screening feature is enabled ('RoamServiceScreeningEnable'=1), then the Tekelec ngHLR proceeds with the PLMN Service Screening and then processes the Location Update as normally with the Subscriber Profile's data as provisioned in the database or with tailored services (See *Service screening while roaming*).

If the PLMN-IMSI validation fails (PLMN and/or IMSI not allowed), then the Location Update is rejected with an operator-defined PLMN reject cause or an IMSI reject cause.

Finally, the mobile service provider can benefit of cost reduction by ensuring that the cost-optimal PLMN/IMSI selection is made when their subscribers are roaming and also by gaining more control in the legal department, for example, in the case a service provider is not allowed contractually to use a given IMSI in a given country.

For more details on the OCPLMN Configuration 'RoamRestrictEnable' parameter and on the operator-defined PLMN reject cause and IMSI reject cause parameters, refer to the "Roaming Controls" section of the (RM-0042) *SDM System Configuration - Reference Manual*.

For instructions on how to enable this feature, define PLMN/IMSI reject causes, provision PLMN Definitions with Node Ranges and OCPLMN Templates, refer to the "Setting Roaming Controls (Operator Controlled PLMN, Roaming restrictions and Service screening restrictions)" section of the *SDM System Configuration-User Guide*.

Service screening while roaming

With the implementation of this feature, the Network Operator can configure multiple service screening restrictions for each Operator Controlled PLMN Template (OCPLMN Template). From the WebCI or CLI or through XML scripts, the Network Operator can define multiple Service Screening Templates and then assign one to each of the OCPLMN Template's roaming PLMNs. This means that f

or each set of roaming PLMN (VLR/GMSC address ranges) assigned to an OCPLMN Template, the Network Operator can assign a Service Screening Template.

Each Subscriber Profile refers to a defined OCPLMN Template, which defines the behavior the Tekelec ngHLR should adopt (Roaming restrictions and Service Screening) when the originating node of UL is belonging to a specific PLMN. In other words the OCPLMN Template lists a set of PLMNs for which specific Roaming Restrictions and Service Screening rules can be defined.

Note: For the "Default PLMN", it is possible to associate different service restrictions, (for example, TeleService, BearerService, Supplementary Service restrictions), for VLR and SGSN node types. It is a general rule that the same PLMN cannot be associated more than one time, but an exception has been made for the "Default PLMN." This exemption means that two entries can be provisioned in the OCPLMN_Data entity with the same "Default PLMN." These two entries must have different Service Screening templates and different Applicable Node Types, which can only be either VLR_Only or SGSN_Only.

Example**:**

OCPLMN Data table:

Entry 1: Default PLMN (Plmn Id=0), Service ScreeningA, NodeType=VLR_Only

Entry 2: Default PLMN (Plmn Id=0), Service ScreeningB, NodeType=SGSN_Only

Entry3: PLMN1 (PlmnId=1), Service ScreeningC, NodeType=VLR_SGSN

With the Service Screening feature, the Network Operator can control the following subscriber services depending on the PLMN in which it is roaming in:

- **CSI Key To Suppress from O-CSI:** CSI Service Keys to be suppressed from the Camel Data in the Subscriber's Profile when the Service Screening Template is applied. The O-CSI to suppress is defined per Service Key, so the CSI suppression is triggered based on the VLR number and the type of the IN service (i.e., the CSI's Service Key).
- **BAOC per BSG:** The list of BAOC BSGs provisioned for a Service Screening Template are added to the Subscriber's explicitly provisioned or not provisioned BAOC when the Service Screening Template is applied. This allows Network Operators, for example, to block outgoing calls in specific countries while still allowing outgoing SMSs. As another example, it also allows Network Operators to force users into USSD-CallBack methods depending on the country in which they are roaming in.

Note: Any BAOC data provisioned in the subscriber's profile remains in the ISD message. The Tekelec ngHLR simply adds the BAOC override mask data to the SS-barring (BAOC BSG) data provisioned in the subscriber profile when building the ISD message.

- **Camel - max Camel Version Allowed**
- **ODB** (All Outgoing, All Outgoing Intl, Premium)

- **TeleServices** (TS91, TS92), **BearerServices** (BS1F, BS17)
- **Other supplementary services** - CLIP, CLIR, COLP, COLR, CW, HOLD, MPTY, REGSUBSCRIPTION (REGIONAL SUBSCRIPTION), CFB, CRNRc, CFNRy.

For each of the Tele/Bearer, ODB and supplementary services , a customized treatment can be configured with a combination of Send/NotSend and Action parameters:

1. Service sent / Service NOT sent to the VLR/SGSN node.
2. If the service is NOT sent, or sent, but reported as "Not Supported by the VLR " in the ISD Response, the following actions can be applied:
   a. Reject Roaming
   b. Send Roaming Restriction Due to Unsupported Feature (RRDUF)
   c. Send BAOC for all BSG except SMS
   d. No Action

If the service is provisioned in the Subscriber Profile the following special treatment is possible:

Table 16: Service screening customized treatment

Send	Action	ISD Req	ISD Rsp - Service Not supported
NO	No Action	The service is dropped from the subscriber profile	Not applicable (the service is not sent - Isd Rsp not relevant)
NO	Reject Roaming	UL Nack - ROAMING NOT ALLOWED	Not applicable (the service is not sent - Isd Rsp not relevant)
NO	Send RRDUF	The Service is dropped and: - If MAP v2/v3 - the parameter RRDUF is included in an ISD and sent to the VLR. - If MAP v1 -as if action = Reject Roaming (UL Nack - ROAMING NOT ALLOWED)	Not applicable (the service is not sent - Isd Rsp not relevant)
NO	BAOC	The Service is dropped and BAOC for all BSGS except SMS is sent to the VLR in an ISD	Not applicable (the service is not sent - Isd Rsp not relevant)
YES	No Action	The Service is sent as provisioned in the Subscriber Profile.	No action
YES	Reject Roaming	The Service is sent as provisioned in the Subscriber Profile.	UL Nack Roaming restricted is sent.
YES	Send RRDUF	The Service is sent as provisioned in the Subscriber Profile.	-If MAP v2/v3 - RRDUF is included in a subsequent ISD - If MAP v1 - as if action = Reject Roaming (UL Nack - ROAMING NOT ALLOWED)
YES	BAOC	The service is sent as provisioned in the Subscriber Profile.	BAOC for all BSG except SMS is sent in subsequent ISDs

At system start-up, the following entries are already created in the database:

- The Service Screening Template 'Not Defined' is created and has no Service Screening rules. By default, an OC PLMN Template's roaming PLMNs refer to the 'Not Defined' Service Screening Template. In order to define Service Screening rules to an OC PLMN Template's roaming PLMN, the Network Operator must assign to it a Service Screening Template provisioned with service rules.
- The Service Screening part of the OCPLMN feature is disabled (RoamServiceScreeningEnabled set to '0'), which means that no service screening restrictions are applied. It can be enabled/disabled dynamically from the CLI, WebCI or using XML, by setting the OCPLMN configuration's 'RoamServiceScreeningEnable' parameter to '1' (enabled) or '0' (disabled).

With the implementation of the Service Screening feature, the ngHLR's Roaming Controls logic has been enhanced with the addition of a Service Screening procedure, which follows the PLMN-IMSI validation procedure for roaming restrictions. After the PLMN-IMSI validation procedure is completed and in the case where the ngHLR concludes that the IMSI is allowed in the roaming PLMN, if the Service Screening feature is enabled, the ngHLR proceeds with the Service Screening procedure and behaves as follows:

- It retrieves the subscriber's Service Screening Template based on the OCPLMN Template of the subscriber and based on the PLMN in which the subscriber is roaming. Note that if the origination node does not belong to any of the PLMNs specified in the OCPLMN Template, the node is considered to belong to the "Default PLMN" of the OCPLMN Template.
- If The Service Screening Template = "Not Defined", no Service Screening is applied and the Update Location processing continues with the Subscriber Profile as provisioned in the database.
- Otherwise the Service Screening Template is retrieved and applied against the provisioned Subscriber's services. The Update Location continues with thus tailored Subscriber Profile, as modified by the service screening rules.

Refer to the "Roaming Controls" section of the *SDM System Configuration - Reference Manual* , for a detailed description of the OCPlmn_ServiceScreenTemplate[ ] entity and its sub-entities (CSISuppress[ ], BAOCBsgOverride[ ], SupplementaryService[ ], BearService[ ], TeleService[ ], ODBService[ ]), which allow the Network Operator to define Service Screening Templates with service screening restrictions.

For instructions on how to enable and provision from the WebCI the OC PLMN feature and the Service Screening Template option, refer to the "Setting Roaming Controls (Operator Controlled PLMN, Roaming restrictions and Service screening restrictions)" section of the *SDM System Configuration - User Guide.*

Support of several OCPLMN templates

The support for multiple OCPLMN Templates allows the operator to define different OC PLMN Templates with a list of 'allowed' roaming PLMNs, to which Roaming restrictions (set of rules for PLMN/IMSI authorizations) and Service Screening restrictions can be defined. Moreover, these OCPLMN Templates can be associated to each subscriber (Primary IMSI) in order to assign a different set of Roaming restrictions and Service Screening restrictions per subscriber. To achieve this, the Network Operator can provision subscriber profiles with an 'OCPlmnTemplateName' (from the WebCI) or an 'OCPlmnTemplateId' (from the CLI), which identifies the OC PLMN Template that should be used for this subscriber.

The Tekelec ngHLR now performs the PLMN-IMSI validation based on the roaming PLMN as well as on the OCPLMNTemplate that is assigned to the subscriber.

OCPLMN Templates can be provisioned through the CLI and WebCI. To use this feature, the operator must do the following:

- Define an OCPLMN Template in the OCPlmn_Template [ ] entity. When creating an OCPLMN Template, a list of roaming PLMNs can be assigned to it and for each of them, a list of "allowed" IMSIs can be defined and a Service Screening Template can be assigned. This OCPLMN Template refers to its Plmn's list of VLRs and their associated set of rules for PLMN/IMSI authorizations and service screening restrictions.
- Assign an OCPLMN Template to a subscriber by provisioning its subscriber profile with the OCPLMN Template Name (from the WebCI) or with the OCPLMN Template ID (from the CLI) of the OCPLMNTemplate you wish to assign to it. The OCPLMN Template that is assigned to the subscriber will be the one used for PLMN/IMSI validation during subscriber registration and for Service Screening validation when processing Update Locations.

Note: At system start-up, an OCPLMN Template with OCPLMN Template Name = "Not Defined" is always created. The Template is used as default for all new subscribers. It is created for the purpose to denote that the subscriber does not have any Roaming restrictions or Service Screening to be applied. By using OCPLMN template = "Not Defined, the feature can be turned OFF on a per subscriber basis. The "Not Defined OCPLMN Template" cannot have any PLMNs assigned to it.

Please refer to the "Setting Roaming Controls (*Operator Controlled PLMN, Roaming restrictions and Service Screening restrictions)"* section of the *SDM™ System Configuration - User Guide* for step-by-step instructions on how to provision this feature. For more detailed information on the parameters used to provision this feature, refer to the "Roaming Controls" section of the *SDM System Configuration - Reference Manual*.

Support of variable length Node (VLR, GMSC) address range

The implementation of the feature that supports a variable length Node (VLR, GMSC) address range has enhanced the Node definition when provisioning the OCPLMN. The field in which the Node Range can be defined has been modified in order to support values of variable lengths, which allows for Node Ranges to be stored as a 1 digit address to a full 15 digit address. For the PLMN validation, the Tekelec ngHLR now uses a "Best-Match" algorithm to match the node address received in the Update Location message with one of the Node ranges defined in the Tekelec ngHLR. The best match for the received Node address corresponds to the longest matching Node Range. The operator can now provision different lengths of Node Addresses for a PLMN when adding a Node (VLR or GMSC) through the CLI and WebCI.

Calculation of affected VLRs following roaming configuration change

When roaming configuration data (i.e. OCPLMN) is changed, it may be necessary for the Tekelec ngHLR to issue a MAP_RESET message since subscriber data at many VLR/SGSN nodes may need to be refreshed. The implementation of this feature adds to the Tekelec ngHLR the capability of calculating the set of VLR/SGSN nodes that would be affected by a change made to the roaming configuration data. Moreover, the implementation of the capability for the Tekelec ngHLR to be able to feed the list of affected VLR/SGSN nodes into its Reset tool, offers to the Network Operator an easy way to configure the Tekelec ngHLR to send a `MAP_RESET` message to the affected VLR/SGSN nodes.

The Network Operator can obtain from the Tekelec ngHLR a list of affected VLR/SGSN nodes for a roaming configuration change, as follows:

- · By executing the 'Compute Plmn Changes' operation for one of the following Plmn Definitions change:
  - Delete Plmn
  - Delete VLR
  - Add VLR
- By executing the 'Compute OCPlmn Template Changes' operation and specifying one of the following OCPlmn Template change:

  - Delete Plmn Reference
  - Delete allowed Imsi
  - Add/delete Service Template Reference

- By executing the 'Compute Service Screening Template Changes' operation and specifying one of the following Service Screening Template change:
  - Modify Service Template (For more information on the service screening template, refer to the description of the 'Service screening while roaming' feature in this document)

Note: The Tekelec ngHLR can calculate the list of affected VLR/SGSN nodes for a single change at a time.

Each operation can be executed from the WebCI, CLI or a XML interface and will produce a list of affected nodes (VLR/SGSN). From the WebCI, a pop-up window will appear and display the list of affected nodes. From the CLI and when using XML files, the OCPlmnNodeNumber entity must be displayed/selected in order to view the list of affected VLR/SGSN nodes last calculated by the Tekelec ngHLR. For a description of the OCPlmnNodeNumber[ ] entity, refer to the "Calculation of VLR/SGSN nodes affected by roaming control changes" section of the *SDM System Configuration - Reference Manual* .

Based on the list of affected VLR/SGSN nodes calculated by the Tekelec ngHLR, the Network Operator can decide to take either one of the following actions by executing the appropriate operation:

- 'Discard': this operation discards the list of affected nodes.
- 'Append': this operation appends the list of affected nodes to the NodeNumberSubset entity's list of nodes (nodes to which the Tekelec ngHLR will send a `MAP_RESET` message upon the execution of the 'Map Reset' operation).
- 'Replace': this operation replaces the NodeNumberSubset entity's list of nodes with the list of affected VLR/SGSN nodes calculated by the Tekelec ngHLR.

Note: Network Operator can at any moment display and edit the current content of the NodeNumberSubset entity as previously implemented.

The Network Operator can make changes to the roaming configuration data as previously implemented and then, if desired, he can execute the 'MAP Reset' operation (also as previously implemented) in order to send `MAP_RESET` messages to the nodes listed in the NodeNumberSubset entity. Keep in mind that the 'MAP Reset' operation must only be executed during low traffic hours.

For more details on these operations, refer to the 'Roaming Controls' section of the *SDM System Configuration - Reference Manual* . For instructions on how to use this feature from the WebCI, refer to the "Calculating the VLR/SGSN nodes affected by a roaming configuration change" section of the *SDM System Configuration - User Guide* .

XML Notifications

The Tekelec ngHLR supports various types of XML (Extensible Markup Language) notifications. It provides an XML interfaces for sending external notifications. This section describes the different XML Notification types that are supported by the Tekelec ngHLR:

- The Roaming Welcome Notifications: the Tekelec ngHLR can be configured to send a notification to an external application (EA) when a subscriber is successfully roaming in a different country or service area. More precisely, the Tekelec ngHLR can be configured to send XML Notifications to an EA when a subscriber undergoes a CC and/or NDC change and/or an IMSI change.

- The VLR Message Notifications: the Tekelec ngHLR can be configured to send a notification to an EA when one of the following MAP message types are received:
  - Location Update
  - Location Update for GPRS
  - Ready SM
  - Purge MS
  - Send Authentication Info (SAI)
  - Cancel Location
- The SS Management Message Notifications: the Tekelec ngHLR can be configured to send a notification to an EA when these types of SS MAP messages are received:
  - RegisterSS
  - EraseSS
  - ActivateSS
  - DeactivateSS
  - InterrogateSS

For more details on each of these features, refer to the following sub-sections. For more details on the XML Interfaces and how to subscribe and activate these notifications, refer to the *SDM XML Notifications - XML Interface Description* document.

Roaming Welcome Notification

The roaming welcome messages feature allows the Tekelec ngHLR to notify a server when it receives a MAP Location_Update or MAP Location_Update_for_GPRS message, with a country code different from the previously registered one. This feature answers to the new requirement of the latest European Union (EU) regulation on roaming tariffs, which requires the operators to notify by SMS their end-users when they roam to a different country.

The Roaming Welcome Notification feature allows the Tekelec ngHLR to detect when end-users roam into a new country and then notify the server that will be in charge of sending an SMS to the user.

New parameters and a table have been created into the Tekelec ngHLR's database to configure this feature. The operator can set this feature to On or Off for the entire Tekelec ngHLR and for each subscriber by specifying its primary IMSI. Moreover, in the new table, a list of Country Codes can be entered for which a notification is not required to be sent by the Tekelec ngHLR. For more details on the different parameters and the table to be configured if using the Roaming Welcome Notification feature, please refer to the "Roaming Welcome Notification" section of the *SDM System Configuration - Reference Manual* and to the "Subscriber Profile (Bearer Services, TeleServices, Call Barring, PreferredRoutingNetworkDomain)" of the *SDM Subscriber Provisioning - Reference Manual* .

For step-by-step procedures on how to provision the new parameters and table of the Roaming Welcome Notification feature, please refer to the "Provisioning Roaming Welcome Notifications" section of the *SDM System Configuration - User Guide* and to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide* in order to turn On/Off this feature for a Subscriber Profile.

The Tekelec ngHLR sends a notification to the server only when all the following conditions are met:

- The country code has changed
- The roaming welcome messages is on for the entire HLR

- The roaming welcome messages is on for the subscriber
- The new country code is not in the list of country codes that doesn't require a notification to be sent for the HLR

Note: The first time an update location is done, no roaming welcome message is sent.

Once the Tekelec ngHLR has detected that the subscriber is roaming in a new country and the conditions to send a notification to the server are met, the "Tekelec XML Subscriber Data Server framework", which provides an XML interface API to the external application server, is used to send the notification, with the following information:

- The local timestamp

XML notifications on NDC change or IMSI change

The XML notifications on NDC change and the XML notifications on IMSI change have been implemented as enhancements of the previously implemented Roaming Welcome Notifications feature.

The Tekelec ngHLR is able to notify a server when it receives a MAP Location_Update or MAP Location_Update_for_GPRS message with:

- A country code different from the previously registered one.
- A country and National Destination Code different from the previously registered one.
- An IMSI different from the previously registered one.

With these enhancements, the following entities and parameters have been implemented and the operator can now provision them through the CLI or WebCI:

- The "RoamingWelcomeMessage" parameter in the HlrConfig entity can be provisioned to either one of the following three states:
  - Off
  - Notify on CC changes or IMSI change
  - Notify on CC-NDC changes or IMSI change

This allows the operator to turn the feature Off or On with notifications sent only when the CC or IMSI change or sent only when the CC-NDC or IMSI change.

- As implemented in the "Roaming Welcome Notifications" feature, the XML notifications can be turned On/Off on a per subscriber (Primary IMSI) basis. To provision this, the operator can set the "SubsRoamingMsgOn" parameter to On/Off in subscriber profiles.
- The RoamingMsgNDCExtractionRule entity can be provisioned to define for a specific CC the method that the Tekelec ngHLR needs to use to extract the NDC. The algorithm used to identify the Country Code of the roamed-to VLR/SGSN is based on the ITU assignment rules. In the case where the Tekelec ngHLR is set to "Notify on CC-NDC changes", the Tekelec ngHLR extracts the CC as per the ITU assignment rules and verifies in the RoamingMsgNDCExtractionRule entity which method is defined for this CC in order to extract the NDC from the VLR GT (e.164 global title). The following are the two methods that have been implemented to extract the NDC from the VLR GT:
  - The "FixedLength" method. With this method, the Tekelec ngHLR finds the NDC digit length defined for the CC and extracts the NDC with the known length.
  - The "NDCList" method. With this method, the Tekelec ngHLR finds the list of NDC for the CC extracted and verifies if the VLR GT NDC is in this list. If it's in this list, the NDC can be extracted from the VLR GT, otherwise the Tekelec ngHLR uses the default CC (CC=0) for which only the

Fixed Length method can be used. This list of NDCs must be defined by the operator manually for a specific Country Code. To define this list, the operator must provision the RoamingMsgNDClist entity with a list of shared country codes and their corresponding NDC list in which roaming welcome messages are sent if the CC-NDC changes.

- The RoamingMsgExeptionCC entity can be provisioned with an exception list of CCs. When the Tekelec ngHLR is set to "Notify on CC changes", the Tekelec ngHLR will never send a notification for the CCs in this list.
- The RoamingMsgExceptionCCNDC entity can be provisioned with an exception list of CCs and NDCs. When the Tekelec ngHLR is set to "Notify on CC-NDC changes", the Tekelec ngHLR will never send a notification for the CC-NDCs in this list. If the operator wishes to restrict an entire country when the Tekelec ngHLR is set to "Notify on CC-NDC changes", the operator needs to enter the Country Code and enter "*" (wildcard) as the NDC.

When the RoamingWelcomeMessage of the Tekelec ngHLR is set to "Notify on CC-NDC changes or IMSI change", the notification is sent under the conditions stated in the following four cases.

First case:

- The roaming welcome messages is ON for the entire HLR
- The roaming welcome messages is ON for the subscriber
- The IMSI for the current registration is different than the IMSI of the previous registration

Second case:

- The current and new VLR GT are not the same
- The roaming welcome messages is ON for the entire HLR
- The roaming welcome messages is ON for the subscriber
- The new CC-NDC of the VLR GT is not in the list of country codes and NDC that doesn't require a notification to be sent for the HLR
- The extracted Country Code has an NDCMethod set to FixedLength
- The extracted CC-NDC (with the length) has changed.

Third case:

- The current and new VLR GT are not the same
- The roaming welcome messages is ON for the entire HLR
- The roaming welcome messages is ON for the subscriber
- The new CC-NDC of the VLR GT is not in the list of country codes and NDC that doesn't require a notification to be sent for the HLR
- The extracted Country Code has an NDCMethod set to NDCList
- The CC-NDC of the New VLR GT is found in the NDCList.
- The extracted CC-NDC (with NDCList) has changed.

Fourth case:

- The current and new VLR GT are not the same
- The roaming welcome messages is ON for the entire HLR
- The roaming welcome messages is ON for the subscriber
- The new CC-NDC of the VLR GT is not in the list of country codes and NDC that doesn't require a notification to be sent for the HLR
- The extracted Country Code has an NDCMethod set to NDCList
- The CC-NDC of the New VLR GT is Not found in the NDCList

Note: The first time an update location is done, roaming welcome message is sent. For the first IMSI change, there is always a notification sent even if the CC or CC/NDC is in the Black list.

Finally, when these conditions are met, the Tekelec ngHLR sends a notification using the "Tekelec XML Subscriber Data Server framework", which provides an XML interface API to the external application server.

For more details on the how the Tekelec ngHLR provides an XML interfaces for sending external notification when a subscriber is successfully roaming in a different country, please refer to the *SDM XML Notifications XML Interface Description* ID-0020 SDM Roaming Welcome Message XML Interface description

For more details on the different parameters and the table to be configured if using this feature, please refer to section *"Roaming Welcome Notification"* of the *SDM System Configuration - Reference Manual* and to section "Subscriber Profile (Bearer Services, Teleservices, Call Barring, PreferredRoutingNetworkDomain" section of the *SDM Subscriber Provisioning - Reference Manual* .

For step-by-step procedures on how to provision the parameters and table of this feature, please refer to the "Provisioning Roaming Welcome Notifications" section of the *SDM System Configuration - User Guide* and to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide* .

VLR Message Notifications

There are two types of VLR Message Notifications

1. VLR XML Notifications
2. VLR Message Notification Log File

VLR Message Notifications (XML notifications on UL UL-GPRS, SAI, Ready SM, Purge MS and CL)

This feature allows the Tekelec ngHLR to notify an external application when it receives the following MAP messages from the VLR (or SGSN):

1. Location Update MAP_UPDATE_LOCATION
2. Location Update for GPRS MAP_UPDATE_GPRS_LOCATION
3. Ready SM MAP_READY_FOR_SM
4. Purge MS MAP_SEND_AUTHENTICATION_INFO
5. Send Authentication Info (SAI) MAP_PURGE_MS
6. Cancel Location

Upon reception of one of these messages, the Tekelec ngHLR generates an XML notification (VlrMessageNotification) and sends it to an external application. Note that a notification is sent when one of these messages is received (i.e. NOT when successfully replied…). The notification therefore provides no information on the result of the MAP transaction. Note however that no notification is sent if the MAP message received is for an unknown subscriber (ex: gprsSubscriptionUnknown).

By default, the VLR message notification feature is unavailable (disabled). This feature is optional and once purchased, the Tekelec *Customer Care Center* can make it available for the Network Operator to activate/deactivate it:

- for the entire system, by provisioning the HlrConfig entity's VlrMsgNotification parameter through the CLI or WebCI.

And

- on a per subscriber basis, by provisioning the SubscriberProfile entity's SubsVlrMsgNotificationOn parameter through the CLI or WebCI.

Note: This feature is based on the same "notification mechanism" used for the "Roaming Welcome Notification" feature and may generate a large number of XML notifications. This will impact the performance and/or decrease the maximum subscriber that can be provisioned on the system. Consequently, this feature must only be enabled on a system that is dimensioned accordingly (for a given capacity AND traffic model). You must contact the Tekelec *Customer Care Center* prior to enabling this feature to prevent any performance issues.

When this feature is enabled for the system and for the subscriber for which the message is received, a XML notification is sent for all Update Locations, GPRS Update Locations, SAI, Ready-for-SM , and Purge MS and Cancel Location messages received from all VLRs.

The "Tekelec XML Subscriber Data Server framework", which provides an XML-based API to the external application server, is used to send the notification, with the following information:

- The local **timestamp**
- The registered **IMSI** of the subscriber
- The "displayed" **MSISDN** of the subscriber
- The **type** of message received (UL or UL_GPRS or SAI or ReadySM or PurgeMS or CL)
- The **global title** (e.164) **address** of the node that sent the message (VLR or SGSN)
- The **Result Notification** with information on whether the message reply was a success or a failure. The supported values are "Successful" and "Fail".

For all message types the following "optional" information is included:

- The **ResultCodeError**. If the Result Notification is "Fail" then the MAP message error message is included in the XML notification message. if the Result Notification is "Successful" then no ResultCodeError is included in the XML notification message.

Depending on the message type, additional "optional" information is included:

- If the type of the message received is UL:
  - The MSC e164 address
- If the type of the message received is ReadySM:
  - The **alert reason** (integer 0)

Note: It is possible for multiple applications to register for VlrMessageNotification. A notification will be sent to each registered application.

It is also possible for VlrMessageNotification and RoamingWelcomeNotification to be used at the same time. This includes:

- The same subscriber enabled for two notifications types, and therefore triggering two notifications from one message (e.g. on UL)
- The same application registering for VlrMessageNotification and RoamingWelcomeNotification
- Different applications registering for VlrMessageNotification and RoamingWelcomeNotification

For details on the VlrMsgNotification parameter, refer to the "HLR Configuration" section of the *SDM System Configuration - Reference Manual*. For details on the SubsVlrMsgNotificationOn parameter, refer to the "Subscriber Profile" section of the *SDM Subscriber Provisioning - Reference Manual* .

For more details on how to activate/deactivate this feature for the entire system, refer to the "Activating/Deactivating the XML notification on UL, UL-GPRS, SAI, Ready SM, and Purge MS and CL" section of the *SDM System Configuration - User Guide* . For more details on how to activate/deactivate this feature for specific subscribers from the WebCI, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Once the Tekelec ngHLR's Roaming Welcome Notification service is configured properly, you can setup the external application (EA) to register. For more details on how to setup the EA to subscribe and activate the Roaming Welcome Notifications service and on how the Tekelec SDM provides an XML-based interface for sending external notification upon reception of UL, UL-GPRS, SAI, Ready SM, and Purge MS and CL MAP messages types, please refer to the SDM XML Notifications - XML Interface Description document

VLR Message Notification Log File

This feature adds a line describing the event to a log file when one of the following types of MAP message is received from the VLR (or SGSN):

1. Location Update
2. Location Update for GPRS
3. Ready SM
4. Purge MS
5. Send Authentication Info (SAI)
6. Cancel Location

The log file is in comma-separated values (CSV) format and is stored on the blade running the Hlr service.

The log file contains the following information:

- The local **timestamp**
- The registered **IMSI** of the subscriber
- The "displayed" **MSISDN** of the subscriber
- The **type** of message received (UL or UL_GPRS or SAI or ReadySM or PurgeMS or CL)
- The **global title** (e.164) **address** of the node that sent the message (VLR or SGSN)
- The **Result**. This indicates if the message was executed successfully or not. In the event of a failure the error code is included:
  - 0=Success
  - Error code is given for other items.
- The **SourceSSN**. This indicates the subsystem number associated with the source code, if it can be determined from the message type. It is one of the following values:
  - 0 = Unknown (set if message is not UL or UL-GPRS)
  - 7 = VLR (only set if message type is UL)
  - 149 = SGSN (only set if message type is UL-GPRS)

Depending on the message type, additional "optional" information is included:

- If the type of the message received is UL:
  - The MSC e164 address
- If the type of the message received is ReadySM:

- The **alert reason** (integer 0)

By default, the VLR message notification log file feature is deactivated. The Network Operator can activate/deactivate it:

- for the entire system, by provisioning the HlrConfig entity's VlrMsgNotification parameter through the CLI or WebCI.

and

- on a per subscriber basis, by provisioning the SubscriberProfile entity's SubsVlrMsgNotificationOn parameter through the CLI or WebCI.

For details on the VlrMsgNotification parameter, refer to the "HLR Configuration" section of the *SDM System Configuration - Reference Manual*. For details on the SubsVlrMsgNotificationOn parameter, refer to the "Subscriber Profile" section of the *SDM Subscriber Provisioning - Reference Manual*.

For more details on how to activate/deactivate this feature for the entire system, refer to the "Activating/deactivating HLR features or functionalities" section of the *SDM System Configuration - User Guide* . For more details on how to activate/deactivate this feature for specific subscribers from the WebCI, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

For more details about VLR Message Notification Log Files, refer to the "VLR Message Notifications Log File" section of the *SDM Monitoring, Maintenance, Troubleshooting - Reference Manual*.

For more details on accessing VLR Message Notification Log Files, refer to the "Accessing VLR Message Notifications Log " section of the *SDM Monitoring, Maintenance, Troubleshooting - User Guide*.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 17: Provisioning Information - VLR Message Notifications

Affected Components	Description	Reference
Provisioning Interfaces	CLI, WebCI, XML Interfaces: XML	
Entities[], attributes	• To enable/disable VLR Message Notifications	*SDM System Configuration Reference Manual*
	• To enable/disable SubsVlrMessageNotificationOn	*SDM Subscriber Provisioning Reference Manual*: • HLR Subscriber Provisioning
Alarms	None	---
Error Messages	None	---

Affected Components	Description	Reference
Counters	None	---
Procedures	• *Configuring the VlrMessage Notification*	*SDM System Configuration User Guide*
	• *Activating the VlrNotificationOpt*	*SDM Monitoring Maintaining Troubleshooting User Guide*
	• *Accessing VLR Message Notification Logs*.	*SDM Monitoring Maintaining Troubleshooting User Guide*: • *Accessing VLR Message Notification Logs.*

XML Notification on SS Management

The XML Notifications on SS Management Messages feature allows an external platform to trigger and execute call forwarding services in the home network. At the same time, this feature enhances call forwarding functionality by allowing end-users to change call-forwarding preferences through their standard handset menus.

Using the handset menus triggers SS management MAP messages (RegisterSS, EraseSS, AcitvateSS, DeactivateSS, InterrogateSS) to the Tekelec ngHLR. The changes are invisible to a visitor network until the Tekelec ngHLR includes the changes in an XML notification to the external platform. Except for the InterrogateSS messages, the SS MAP messages are forwarded directly from the Tekelec ngHLR to all call forwarding services.

InterrogateSS messages are forwarded only to Call Forwarding Unconditional services. The InterrogateSS message for other call forwarding services is handled by the VLR and remains invisible to the Tekelec ngHLR.

The XML Notifications on SS Management Messages feature provides significant cost savings to the mobile service provider through optimal routing without relying on the visited network. The feature:

- avoids international loopbacks of calls diverted to voice mail.
- prevents the visited network to route diverted calls and charge long distance or international fees.
- allows the operator to provide full Call Forwarding Unconditional (CFU) and Conditional Call Forwarding (CCF) functionalities to its subscriber base with significantly reduced fraud risk.
- adds the ability for end-users to use normal handset menus to change call forwarding settings.

The XML notification is done through a database request, which returns all SS MAP parameters of the message in addition to some subscriber information. Multiple servers can register for the "SSMgmt notification". Each server will receive all notifications.

The feature provisions multiple IMSI ranges through a Tekelec ngHLR database table called "HlrSSIMSIRange".

The configuration is made on an IMSI range. Multiple ranges can be defined within existing provisioned IMSI ranges in the Tekelec ngHLR configuration. The feature is configured by setting these flags:

- Global feature flags are located in the HlrConfig table:

  - The HlrSSMgmtFeature flag activates and deactivates the feature, and makes it unavailable. Activation and deactivation are dynamic (no restart of HLR services required).

- IMSI range flags are located in the HlrSSImsi table:
  - The Notify flag enables or disables the feature on a specific IMSI range. To check this flag, the global feature flag has to be active.
  - The suppression flag indicates whether to store the information in the Tekelec ngHLR. To check this flag, the Notify IMSI Range for this range has to be active.
  - The Reject flag indicates whether to notify InterrogateSS messages. To check this flag, the Notify IMSI Range for this range has to be active.

The SS MAP notification includes this information:

- The Subscriber MSISDN number or Display associate.
- The Subscriber IMSI number, Register IMSI.
- The VLR number.
- The SS message code service.
- The SS message type.
- No reply conditional timer, taking values from 5 to 30.
- Forward to number, telephone number.
- Forward to number with subaddress, telephone number.
- The Long Number supported.
- Basic service groups associate to message. This corresponds to BS (Bearer services) and TS (Tele services).
- The date and time when the message is sent (year - month - day - hour - minutes - seconds).
- Interrogate message Error - included only when the SS map message is an Interrogate msg.

HLR Number Configuration

The HLR Number Configuration feature allows a network operator to configure the Tekelec ngHLR with multiple HLR numbers. This enables the HLR to manage subscribers from various PLMN (Public Land Mobile Networks). Each HLR number belongs to a different PLMN and is associated with a specific range of IMSI values. The proper HLR number is used for routing MAP transactions depending on the IMSI involved in the transaction. The proper HLR number is also used in determining the roaming status of the subscriber.

Multiple IMSI range per HLR

The Database of the Tekelec ngHLR allows more than one IMSI range to be defined per HLR. Each HLR number can be associated to multiple ranges of IMSI values.

Multiple IMSI range can now be configured via the CLI and WebCI for each HLR number configured.

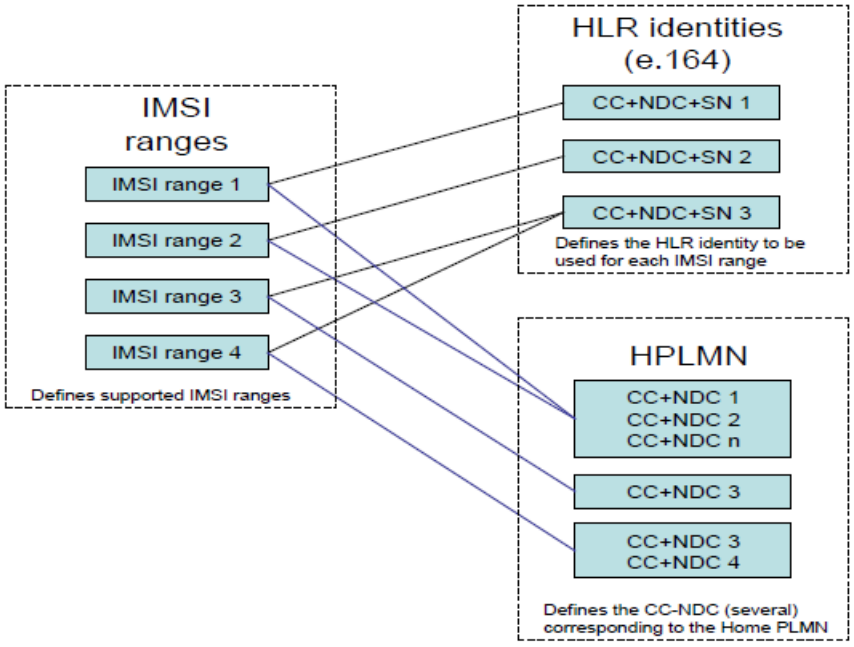
Support for multiple CC-NDC as Home PLMN

This new feature has been implemented to provide more flexibility in defining the HPLMN CC and NDC, and in defining the HLR identity per IMSI range. It provides support to networks with more than one CC-NDC as their HPLMN.

The Multiple CC-NDC feature provides for the possibility to decouple the definition of the HLR identity and the definition of the Home PLMN. In addition it gives the possibility to define the Home

PLMN as a set of up to 100 CC-NDC combinations. The operator can define the HLR identity and the Home PLMN for each of their IMSI ranges. Moreover, the operator has the flexibility of defining the same HLR identity and/or the same definition of Home PLMN for different IMSI ranges.

To define HLR identities, define HPLMN definitions and provision each of them with a list of CC-NDC combinations (multiple CC-NDC as Home PLMN) and to define the IMSI Ranges supported by the HLR and associate them with an HLR identity and HPLMN definition, three tables must be configured either through the WebCI or CLI. Please refer to the *Define HLR identities, HPLMN definitions and IMSI Ranges* section of the *SDM System Configuration - Reference Manual* for more details on these tables and their attributes. For step-by-step instructions on how to provision these tables, refer to the *Defining PLMNs, Multiple Home PLMNs and HPLMN Countries* section of the *SDM System Configuration - User Guide* .



Upon reception of a UL or GPRS_UL, the HLR now uses the HPLMN definition to define the roaming status of the subscriber, instead of using the HLR e.164 address.

If the HLR identities and the HPLMNs for the operator's IMSI ranges are defined as on the graphic above, a subscriber with IMSI in IMSI range 4 will be considered roaming out of HPLMN, if the VLR from which he registers is with CC+NDC combination different than CC3+NDC3 or CC4+NDC4. He will be considered roaming out of HPLMN Country (international roaming), if the VLR from which he registers has CC different than CC3 and CC4. If the CC of the VLR is the same as CC3 or CC4, but the NDC of the VLR is different from the HPLMN NDC3 or NDC4, the subscriber is considered roaming within the HPLMN Country (national roaming).The source address of the HLR included in the messages sent back to the VLR will be CC3+NDC.

Support for multiple Home PLMN Country Definitions

This feature allows the operator to provision multiple HPLMN Country definitions for each IMSI range. It provides full flexibility in the definition of the HPLMN and HPLMN Country. The HPLMN and HPLMN Country definitions can now be configured through the CLI and WebCI as two completely separate and independent lists. This allows the operator to define its nodes in whatever combination of HPLMN and HPLMN Country Nodes. The operator is now able to define the HLR identity, the

HPLMN (list of CC-NDC combinations) and HPLMN Country (list of CCs) for each of the IMSI ranges defined. Moreover, the operator now has the flexibility of defining the same HLR identity and/or the same definitions of HPLMN and/or HPLMN Country for different IMSI ranges. Following the same logic used to determine whether the subscriber is roaming outside the HPLMN or not, the Tekelec ngHLR now uses the IMSI's HPLMN Country list to determine whether or not the subscriber is roaming outside HPLMN Country.

In order to define lists of CCs for the HPLMN Country and assign them to an IMSI range, the operator must provision the following new table and parameter, either through the WebCI or CLI:

- The HPLMN Country table, which allows to provision multiple HPLMN Country definitions (list of CCs).
- The HplmnCountry parameter in the IntraPlmnImsiRange table, which allows to assign a HPLMN Country definition, along with an HLR identity and HPLMN definition, to a specific IMSI range.

Please refer to the *"Define HLR identities, HPLMN definitions and IMSI Ranges"* section of the *SDM System Configuration - Reference Manual* for more details on these tables and their attributes. For step-by-step instructions on how to provision these tables, refer to the "Defining PLMNs, Multiple Home PLMNs and HPLMN Countries" section of the *SDM System Configuration - User Guide*.

FTN Digits Analysis

When subscribers register their Call Forwarding service, they can optionally input a "Forward-To Number" (FTN). The FTN is relayed to the Tekelec ngHLR from the MSC in the MAP messages, with the "Nature of Address" (NOA) indicator set to international, national or unknown. With the implementation of the new FTN Digits Analysis feature, the Tekelec ngHLR is able to convert the FTNs with the NOA set to 'international', 'national' and 'unknown' and always store them in international format, as per 3GPP Specifications.

With this new feature, the operator has to define in the Tekelec ngHLR the following three parameters for each instance (i.e., for each IMSI range supported on the Tekelec ngHLR):

- **IDD** (International Direct Dialing) = Prefix dialed to call FROM that country TO a different country, equivalent to the '+' sign.
- **NDD** (National Direct Dialing) = Prefix dialed to call within a country.
- **CC** (Country Code) = Prefix dialed to call TO that country.

For more details on these parameters, please refer to the "Forward-To-Number (FTN) rule Provisioning for FTN Digits Analysis" section of the *SDM System Configuration - Reference Manual*. The IDD, NDD and CC parameters can all be configured via the CLI or WebCI. Please refer to the "Creating HLR identity(ies) by defining HLR Addresses" section of the *SDM System Configuration - User Guide* for step-by-step procedures on how to configure them from the WebCI.

With the FTN Digits Analysis feature, the Tekelec ngHLR analyses the FTN provided in the RegSS message and either accepts it and stores the FTN in the international format or refuses the RegSS message and doesn't store the FTN. Here is the logic followed by the Tekelec ngHLR when analyzing the FTN provided in the RegSS message and the sequence in which it is followed:

- If the FTN matches exactly one of the special numbers defined in the Tekelec ngHLR's database, the RegSS is refused and the FTN is not stored in the database.
- If the FTN matches exactly one of the short numbers defined in the Tekelec ngHLR, the RegSS is accepted and the Tekelec ngHLR follows the translation rule defined in the database in order to store the FTN as a long number in international format.

- Else the Tekelec ngHLR normalizes the FTN provided in the RegSS into an international format, as follows:
  - If the NOA is set to international: the Tekelec ngHLR keeps the FTN as received.
  - If the NOA is set to national, the Tekelec ngHLR accepts the RegSS message and transforms it in international format by applying the following:
    - If the supplied FTN matches an exception rule
      - Apply Exception rule
      - Add CC
      - Keep resulting FTN
    - Else
      - If supplied FTN matches HLR defined NDD
        - Suppress NDD
        - Add CC
        - Keep resulting FTN
  - If the NOA is set to unknown
    - If the supplied FTN matches a short number translation rule
      - Translate FTN per rule
      - Keep resulting FTN
    - Else
      - If first digits = NDD
        - If National Exception Rule matching
        - apply exception rule
      - Else
        - Suppress NDD
      - Add CC
    - Else
      - If First digits = CC
        - keep as received
      - Else
        - Add CC
- If the FTN (now in international format) is part of the global "black-list" (Restricted FTN) defined in the database, the Tekelec ngHLR refuses the RegSS and doesn't store the FTN.
- Else

- If the subscriber has an assigned FTN Management Rule, the Tekelec ngHLR checks if the FTN is part of the "white-list" of the assigned rule. If it is part of the "white-list", the RegSS is accepted and the FTN is stored in the database.
- Else the RegSS is refused and the FTN is not stored in the database.

When the Tekelec ngHLR determines a FTN to be valid after the logic above is completed, it always stores it in international format and includes it in the ISD message.

In the algorithm presented above, for the conditions verifying a match of the FTN provided in the RegSS with the following:

- A special number, refer to *FTN Special numbers* in this document.
- A short number defined with a translation rule, please refer to *Short number translation on RegSS (FTN Translation Rule)* in this document.
- A national exception rule, refer to *FTN Exception rules* in this document.
- The Tekelec ngHLR's "" or the subscriber's FTN management rule "white-list", refer to the following section "" of this document.

FTN Special numbers

The Tekelec ngHLR allows a list of specific disallowed numbers to be stored (e.g. 911, 112, etc). This means that the Network Operator can define special numbers that can never be Forward-To-Numbers. In the analysis of the FTN, the Tekelec ngHLR verifies if there is an exact match between the FTN provided in the RegSS and the special numbers defined in the database. If there is an exact match, the Tekelec ngHLR refuses the RegSS with the FTN provided.

Refer to *FTN Digits Analysis* for a description of the FTN Digits Analysis implemented in the ngHLR and for details on when this special number verification is applied.

The Network Operator can define these special numbers from the WebCI, by provisioning the FtnSpecialNumbers entity. For more details on the FtnSpecialNumbers entity and its parameters, refer to the "Forward-To-Number (FTN) rule Provisioning for FTN Digits Analysis" section of the *SDM System Configuration - Reference Manual*.

For step-by-step instructions on how to provision special numbers through the WebCI, refer to the "Defining FTN Special numbers" section in the *SDM System Configuration - User Guide*.

FTN Exception rules

The operator can provision some exception rules in the FTN formats and replace some prefixes with a substitute number that will ensure that the Tekelec ngHLR stores the FTN in the correct international format.

Refer to the *FTN Digits Analysis* for a description of the FTN Digits Analysis implemented in the Tekelec ngHLR and for details on when these exception rules are applied.

The Network Operator can define some exception rules from the WebCI, by provisioning the FtnExceptionRules entity. For more details on the FtnExceptionRules entity and its parameters, refer to the " Forward-To-Number (FTN) rule Provisioning for FTN Digits Analysis" section of the *SDM System Configuration - Reference Manual*.

For step-by-step instructions on how to provision exception rules through the WebCI, refer to the "Defining FTN Exception rules" section in the *SDM System Configuration - User Guide*.

Short number translation on RegSS (FTN Translation Rule)

Subscribers may provide a short number (e.g. voice mail access number) or a national format as a "Forward-To Number" (FTN) when activating or registering their Call Forward service. Short numbers can include specific formats, national formats may vary from country to country and in some cases the NDD prefix makes part of the number for certain types (e.g. in Italy NDD=0, the international format for fixed numbers is IDD_NDD_Number, while it is IDD_Number for mobile numbers).

The Short number translation on RegSS feature is implemented to ease the use of the Call Forwarding service for the subscriber by allowing him to enter short numbers and any national numbers and to increase the successful calls ratio. The Tekelec ngHLR includes a logic that will analyze received FTNs in Supplementary Service Registration messages and will apply a set of predefined and configured rules. The logic takes into consideration the received Nature of Address (NOA) and the configured CC, IDD, NDD for the Home network.

In fact, this feature builds on the "FTN Digits Analysis" feature in order to enable the translation of short numbers and in order to properly store into international a NOA set to national or unknown in the case where it represents an exception. For this feature, the Tekelec ngHLR introduces two new tables in order to provide a mean to provision translation rules for short numbers per HLR instance, i.e. for each IMSI range and in order to provision exception rules for National format per HLR instance, i.e. for each IMSI range.

Please refer to the "Forward-To-Number (FTN) rule Provisioning for FTN Digits Analysis" section in the *SDM System Configuration - Reference Manual* for more information on the parameters of the following new tables: HlrFtnProvisioning, HlrFtnTranslationRules and HlrFtnExceptionRules. For step-by-step procedures on how to provision these tables, please refer to the "Defining FTN Short Number Translation Rules on RegSS" section of the *SDM System Configuration - User Guide*.

Enhanced FTN Management (FTN Management Rule)

The "Enhanced FTN Management" feature allows the operator to manage Forward-to-number (FTN) rules per subscriber and to globally restrict some specific FTN (black-list).

With this feature, the operator can define different lists of allowed FTN(s) (white-list), where each list corresponds to a "FTN Management Rule", and can also assign each subscriber with one "FTN Management Rule" in its subscriber profile. A Tekelec ngHLR configured with this feature, will accept or refuse the registration of an FTN performed by a subscriber with a RegSS/ActSS, depending on the "FTN Management Rule" (the allowed FTN list) that is assigned to its subscriber profile. This allows the operator to better control the registration of the FTN(s) for each subscriber.

With this feature, the operator can also choose to globally restrict some FTNs (for all subscribers) by defining a global list of restricted FTNs (black-list) in the Tekelec ngHLR configuration. With the configuration of such a list, the Tekelec ngHLR doesn't accept subscribers to register a FTN (with RegSS/ActSS) that is in the restricted FTN list (black-list).

Finally, with the Tekelec ngHLR configured with this feature, when it receives a RegSS/ActSS from one of its subscribers, the FTN is refused if It is define in the "Restricted FTN" list (black-list) or if the subscriber has a "FTN Management Rule" (white-list) and the FTN is not defined in the list of allowed FTN. Otherwise, the Tekelec ngHLR accepts the FTN registered from the subscriber with a RegSS/ActSS.

This feature can be provisioned by the operator through the WebCI and CLI interfaces. The following can be provisioned:

- The "Restricted FTN" list (black-list) can be defined in the RestrictedFTN entity.
- Different "FTN Management Rules" can be defined in the FTNManagementRule entity and for each of these rules, the corresponding list of allowed FTNs can be provisioned in the AllowedFTN entity.

- The "FTNRule" parameter (called FTNManagementRule in the WebCI) can be provisioned in order to assign a "FTN Management Rule" to a subscriber.

The "FTN Management Rule" and "Restricted FTN" list do not apply in the case where the FTN is provisioned by the operator through the WebCI or CLI. They only apply for a registration of a FTN from a subscriber with a RegSS/ActSS.

In addition to these entities, a counter "Number_of_RESTRICTED_FTN" has been implemented for this feature in order to count the number of times an FTN is refused because it is in the globally restricted FTN list (black-list).

For more detailed information on the RestrictedFTN, FTNManagementRule and AllowedFTN entities that have been implemented with this feature, refer to the "Forward-To-Number (FTN) rule Provisioning for FTN Digits Analysis" section in the *SDM System Configuration - Reference Manual*. For more details on the FTNRule (aka FTNManagementRule) parameter implemented in the SubscriberProfile entity for the HLR application, refer to the "SubscriberProfile (Bearer Services, Teleservices, Call Barring, PreferredRoutingNetworkDomain)" section of the *SDM Subscriber Provisioning - Reference Manual*. For more details on the "RestrictedFTN" counter, refer to the *SDM Performance Measurements* document.

For step-by-step instructions on how to provision these entities and parameter, refer to the "Provisioning Forward-To-Number rules for FTN Digits Analysis" section in the *SDM System Configuration - User Guide*.

Multiple CSI phase provisioning

This feature separates the provisioning of CAMEL phase 1, 2, 3 with multiple TDPs by allowing the Network Operator to provision multiple CSIs with different Camel Phases and multiple TDPs per phase for O-CSI and T-CSI. All other CSI types can only have one phase provisioned for them. To achieve this, the CamelPhase parameter has been included as part of the primary key of the HlrCamelCsiData entity.

Moreover, CSI selection rules have been added to precede the message handling procedure. A CSI is selected based on these CSI selection rules only if the following conditions are met:

- For Update location (O-CSI only):
  - O-CSI is provisioned with provisionState = ON
  - At least one DP (collected Info for camel phase < 3) is provisioned and the DP has the provisionState=ON
- For SRI (T-CSI and O-CSI):
  - CSI is provisioned with provisionState = ON
  - CSI is provisioned with activeState = ON
  - At least one DP is provisioned (O-CSI: collected Info for camel phase < 3) and the DP has the provisionState = ON

The CSI selection rules consist in the following:

- The Tekelec ngHLR now searches through all of the subscriber's provisioned O-CSIs/T-CSIs and compares each of their Camel Phase with the VLR/SGSN Camel Phase.
- The Tekelec ngHLR will select the CSI with the closest Camel Phase to the VLR/SGSN's Camel Phase, as follows:
  - In the case where a CSI's Camel Phase equal to the VLR/SGSN Camel Phase is found, this CSI is selected.

- In the case where no Camel Phase equal to the VLR/SGSN Camel Phase is found, the Tekelec ngHLR behaves as follows:
  - If one or more Camel Phases lower than the VLR/SGSN Camel Phase are found, the CSI selected is the one with the highest Camel Phase (the highest still being lower than the VLR/SGSN Camel Phase).
  - Otherwise, if one or more Camel Phases higher than the VLR/SGSN Camel Phase are found, the CSI used is the one with the lowest Camel Phase (the lowest still being higher than the VLR/SGSN Camel Phase.
  - Otherwise, no CSIs are provisioned for this subscriber.

Once the CSI has been selected, the Tekelec ngHLR follows the CAMEL handling messaging procedure using this CSI and its provisioned Camel Phase.

See *Enhanced CAMEL handling* for a description of the Tekelec ngHLR's behavior when handling messages for a subscriber provisioned with O-CSI.

Enhanced CAMEL handling

With the implementation of the "Enhanced CAMEL handling" feature, intelligence has been added to the Tekelec ngHLR when handling CAMEL.

When a subscriber is provisioned with CAMEL O-CSIs (flags) and an UpdateLocation is received for this subscriber, the Tekelec ngHLR must check which CAMEL Phase is supported by the VLR or SGSN initiating the request. Depending on the supported CAMEL Phase, the HLR will include and encode the O-CSIs in the 'InsertSubsData' message.

In the previous implementation, the Tekelec ngHLR behaved in this manner:

- Situation A: If the VLR/SGSN supported CAMEL Phase is the same as the Subscriber O-CSI, then the Tekelec ngHLR sends the O-CSIs as they are provisioned.
- Situation B: If the VLR/SGSN supported CAMEL Phase is lower than the Subscriber O-CSI, then the CSI downgrades the O-CSIs, if they exist in the lower CAMEL phase.
- Situation C: If the VLR/SGSN does not indicate CAMEL support, the Tekelec ngHLR doesn't send any O-CSI in the ISD message.

In the current implementation, the Tekelec ngHLR still behaves as described above with the addition of enhanced behaviors that have been implemented to provide more flexibility and options in situations B and C. The Tekelec ngHLR now behaves as follows:

Table 18: ngHLR behavior for enhanced CAMEL handling

State	A	B	C
Camel Phase/ Action	VlrPhase = 0	VlrPhase < CsiPhase	VlrPhase >= CsiPhase
Standard	The Tekelec ngHLR doesn't send the O-CSI.	The Tekelec ngHLR downgrades the O-CSI phase.*	The Tekelec ngHLR sends the O-CSI without applying any "Action".

Deny	The Tekelec ngHLR rejects the Update Location.	The Tekelec ngHLR rejects the Update Location.	
ODB-BAOC	The Tekelec ngHLR doesn't send the O-CSI. The Tekelec ngHLR adds "Barring of All Outgoing Calls" to the ISD message.	The Tekelec ngHLR downgrades the O-CSI phase* and adds "Barring of All Outgoing Calls" to the ISD message.	
Apply Mask	The Tekelec ngHLR doesn't send the O-CSI. The Tekelec ngHLR suppresses the Bearer Services/Teleservices (operator-defined) provisioned for this subscriber: - Subscriber profile	The Tekelec ngHLR downgrades the O-CSI phase* and suppresses the Bearer Services/Teleservices (operator-defined) provisioned for this subscriber: - Subscriber profile - Camel TDP	
BSG-BAOC	The Tekelec ngHLR doesn't send the O-CSI. The Tekelec ngHLR adds "Barring of All Outgoing Calls" to the ISD message for all the provisioned BSG except SMS.	The Tekelec ngHLR downgrades the O-CSI phase* and adds "Barring of All Outgoing Calls" to the ISD message for all the provisioned BSG except SMS.	

*The expression "Downgrade O-CSI phase" means that only the services that are supported in the VLR/SGSN Camel Phase are sent in the ISD message.

The Action is currently implemented only for OCSI. For OCSI the action is applicable on UL only.

With this feature, the operators can control the CAMEL behavior, on a per-subscriber basis, when they are roaming outside of their network.\

For example, with this feature, the operators can:

- Prevent Prepaid subscribers to use any service when out of CAMEL coverage
- Block outgoing calls (but not incoming calls) when roaming on non-CAMEL VLRs
- Block MO-SMS while roaming on CAMEL Ph1 VLRs

The operator can configure the four Tekelec ngHLR behaviors described above, by provisioning the following through the CLI and WebCI:

- The "ActionOnUnsCamelPh" parameter can be provisioned on a per-subscriber basis in the "CamelCsiData" entity. This allows the operator to determine the type of action (behavior) it wants the Tekelec ngHLR to take when handling CAMEL.

The operator can configure each CAMEL-subscriber (subscriber with CAMEL services provisioned) with one of the following behaviors:

- 0 (standard and previous behavior): The Tekelec ngHLR doesn't send any CSI in the ISD message.
- 1 (Deny): The Tekelec ngHLR rejects the Update Location.
- 2 (ODB): The Tekelec ngHLR sends the "Barring of All Outgoing Calls" in the ISD message.
- 3 (Apply Mask > TS/BS suppression): The Tekelec ngHLR applies the Mask (operator-defined) and suppresses some specific BS/TS provisioned for the subscriber.
- 4 (BSG-BAOC): When this action is selected for a subscriber's O-CSI, the Tekelec ngHLR sends BAOC for all provisioned BSGs except SMS.

When the value "Apply Mask" is chosen, at least one TS/BS Mask template needs to be provisioned. The ServiceMaskTemplateName parameter implemented in the Subscriber Profile entity allows the operator to specify to which TS/BS Mask template the Tekelec ngHLR must refer to when handling CAMEL for a specific subscriber. This allows different subscribers to have different TS/BS masks. This mask is then used by the Tekelec ngHLR to calculate the list of TS/BS to be sent in the ISD message.

The "CamelServiceMaskTemplate" entity has been implemented with this feature to allow the operator to define TS/BS mask templates. For a subscriber with ActionOnUnsCamelPh = 'Apply Mask', the Tekelec ngHLR will apply to the list of services (TeleServices or BearerServices) the TS/BS mask provisioned in the template to which the subscriber refers to.

If the mask is empty, then all specified BS/TS are sent out. There are 2 sets of TS/BS lists to which the mask can be applied:

- Subscriber Profile: These lists are directly associated with a subscriber and the services it is entitled to. They are provisioned for each subscriber in the "SubscriberProfile" entity.
- Camel TDP: These lists are linked to a specific Camel Triggering Detection Point (TDP). In the context of this feature, we only support the O-CSI TDP, and the associated BS/TS lists. They are provisioned in the "CamelCsi_DP" entity.

The following two counters have also been implemented with this feature:

- The "Number_of_Rejected_Update_Location" counter counts the number of UL messages that have been rejected by the Tekelec ngHLR as a result of non-CAMEL support ("Deny").
- The "Number_of_ODB_on_UL" counter counts the number of ODB sent back in the ISD message as a result of non-CAMEL support ("ODB").

Moreover, the Tekelec ngHLR sends a Cancel Location to the VLR in the following conditions:

- The CSI Action has changed to "Deny".
- The CSI Camel Phase has changed from situation C to situation B and the CSI Action is set to "Deny".

Finally, it is important to take note that this feature supersedes the *T-CSI Suppression* feature.

For more information on the parameter and entity implemented in this feature, refer to the "Camel services" section of the *SDM Subscriber Provisioning - Reference Manual* . For step-by-step instructions on how to provision this parameter and entity through the WebCI, refer to the "Provision Camel services for a subscriber" procedure in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Enhanced propagation of implicit subscriber data changes

With this feature, the following capabilities have been added to the Tekelec ngHLR's Camel Roaming and Operator Controlled PLMN logics in order to enhance the propagation of subscriber data changes from the Tekelec ngHLR to the VLR/SGSN:

- The capability to send a message (ISD, DSD, CancelLocation) to the VLR/SGSN in order to update it in the cases where the O-CSI's "ActionOnUnsCamPh" transitions from or to "BSG-BAOC". Such a transition can be the result of one of these following changes:
  - deleting/unprovisioning or adding another CamelPhase of the O-CSI
  - changing the O-CSI's 'ActionOnUnsCamPhase' from or to "BSG-BAOC"

In the cases where the change in a subscriber's O-CSI data results in one of the action changes shown in the table below, the Tekelec ngHLR sends an ISD/DSD/CancelLocation message to the VLR/SGSN, as needed.

Table 19: O-CSI action changes

Type of O-CSI change	Prior to O-CSI change	After O-CSI change	Messages sent by the Tekelec ngHLR
	Action taken by the Tekelec ngHLR for O-CSI as per the 'ActionOnUnsCanPh' configuration		
A	None *(The Camel Phase supported by the VLR is >= Subscriber's O-CSI CamelPhase)*	'BSG-BAOC' action applied	ISD for BAOC *
A or B	'Standard' action applied	'BSG-BAOC' action applied	ISD for BAOC*
A or B	'ODB' action applied	'BSG-BAOC' action applied	ISD for BAOC*
A or B	'Apply Mask' action applied (TS/BS suppression)	'BSG-BAOC' action applied	ISD for BAOC*
A	'BSG-BAOC' action applied	None *(The Camel Phase supported by the VLR is >= Subscriber's O-CSI CamelPhase)*	ISD or DSD for BAOC*
A or B	'BSG-BAOC' action applied	'Standard' action applied	ISD or DSD for BAOC*
A or B	'BSG-BAOC' action applied	'Deny' action applied	Cancel Loc
A or B	'BSG-BAOC' action applied	'ODB' action applied	ISD or DSD for BAOC*
A or B	'BSG-BAOC' action applied	'Apply Mask' action applied (TS/BS suppression)	ISD or DSD for BAOC *

Note: *The need for sending an ISD/DSD message for BAOC is always reevaluated. Whether an ISD/DSD message is sent or not for adding/removing BAOC BSGs depends not only on the change of the action, but also on the following:

- Whether those BAOC BSGs are still applicable for other features
- Whether the O-CSI induced BAOC BSGs (BAOC BSGs sent to the VLR that are not part of the BAOC as provisioned in the subscriber profile) have been already sent in previous ISDs, by:
  - Service Screening Template

    Or
  - Subscriber's provisioned CUG, if the VLR/SGSN does not support CUG - the induced BSGs depend on the provisioned CUG.

To determine whether the VLR/SGSN has to be updated with a newly "induced BAOC BSG" the Tekelec ngHLR must be able to distinguish whether this BAOC BSG has not been already induced by another feature and sent already to the VLR/SGSN. For this purpose, the "InducedBaocVlr" and "InducedBaocVlrServScr" (Service Screening Induced BAOC BSGs) fields have been implemented in the Subscribers' Volatile Data to keep track of the induced BAOC BSGs that have already been sent to the VLR. By knowing which BAOC has been induced, the Tekelec ngHLR can determine whether a removal or addition of the O-CSI induced BAOC BSGs would require an update of the BAOC (ISD/DSD messages) in the VLR/SGSN.

For more details on the "ServScrInducedBaocVlr" field in the Volatile data, refer to the "HLR Volatile Data" section in the *SDM Subscriber Provisioning - Reference Manual*. You can display the HLR Volatile Data from the CLI, see the CLI Navigation path in the "HLR Volatile Data" section.

- The capability to detect a change of the subscriber's reference to OCPLMN Template and Cancel the subscriber's registration in the current VLR/SGSN, if the newly assigned subscriber's OCPLMN Template restricts the roaming in his current PLMN. In other words, when changing the subscriber's OCPLMN template association (OCPlmnTemplateName) from one template to another, the roaming restrictions applicable for the subscriber's current location are re-evaluated. If the newly assigned OCPLMN Template restricts the roaming in the current VLR/SGSN, the Tekelec ngHLR triggers a Cancel Location message.

System Default call handling (DCH) override

This feature has been implemented in order to override the default call handling (DCH) option (continue call or release call) provisioned by the Network Operator in a specific subscriber profile's TDP of the CAMEL Subscription Information.

This allows the Network Operator to set at a global level (for all subscribers and all messages) the default call handling to one of the following options:

- Use per-subscriber DCH setting - the normal setting. This option is the equivalent of having the System DCH override feature disabled.
- Use DCH "continue" for all messages: this option allows the calls to continue even if the SCP is unavailable. This prevents calls from failing when the SCP node is not reachable.
- Use DCH "release" for all messages: with this option, the communication is not established if the SCP is unavailable.

To set these options, the Network Operator can provision the global DCH Override flag: DCHOverride in the HlrCamelConfig entity of the HLR's database. This flag can be dynamically modified during running-time of the system and overrides the setting of the TDP CSI's DefaultCallHandling parameter provisioned on a per-subscriber basis. Take note that this parameter does not change the subscriber data settings in the HLR's database. It simply overrides the DCH value for all the following CSI types sent as part of ISD and SRI MAP operations: O-CSI, T-CSI, VT-CSI, GPRS-CSI, OSMS-CSI, D-CSI.

The system DCH override feature applies to any CSI included in any message generated by the Tekelec ngHLR. It applies only if the message includes some Camel information, otherwise the global DCH value has no impact. Moreover, with this implementation, the global DCH flag will apply automatically to any new MAP message added to the Tekelec ngHLR.

The Tekelec ngHLR doesn't send incremental ISD messages to the network when the DCH override value changes. Once the parameter is changed (i.e. before and after the SCP upgrade/outage), the Network Operator must send manually a MAP Reset message to one or more VLR nodes if necessary, in order to propagate the new information related to Camel-DCH. Refer to the MAP Reset feature described below.

For more information on the HlrCamelConfig entity and the DCHOverride parameter implemented in this feature, refer to the "Camel Configuration" section of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision this parameter and entity through the WebCI, refer to the "Provisioning CAMEL" section in the *SDM System Configuration - User Guide*.

Support of PLMN Specific Supplementary Services in SRI_ack

The Tekelec ngHLR supports PLMN Specific Supplementary Services. This feature allows the operator to provision supplementary service codes (among the possible codes from F1 to FF) for any PLMN Specific Supplementary Services (such as Ring-back Tone service) in the subscriber's Supplementary Service profile. The Tekelec ngHLR simply sends the PLMN Specific Supplementary Service provisioned for the subscriber in the Send Routing Information acknowledgement.

For the step-by-step procedures to provision these codes, please refer to the "Viewing/Editing a HLR Service Profile" section in the SDM Monitoring, Maintaining, Troubleshooting - User Guide. For details on the parameters to be provisioned, please refer to the "PLMN Specific Supplementary Services Provisioning" section and to the "PLMN Specific Supplementary Services Basic Service Group" section in the *SDM Subscriber Provisioning - Reference Manual*.

Call Forwarding Default (CFD)

For a subscriber that has deactivated the Conditional Call Forwarding services that are provisioned in its GSM profile in the Tekelec ngHLR, the Mobile Terminated calls directed to this subscriber fail. The Call Forwarding Default feature solves this problem and enhances the network call setup failure ratio by allowing the operator to supply a default forward-to-number (FTN).

This Default FTN is enabled by default and becomes active whenever the subscriber tries to deactivate a Conditional Call Forwarding service.

Please refer to the "Viewing/Editing a HLR Service Profile" section in the SDM Monitoring, Maintaining, Troubleshooting - User Guide for step-by-step instructions on how to provision a Default FTN for the CCF services per subscriber. For more detailed information on the parameters used to provision this feature, refer to the "Call Forward" section in the *SDM Subscriber Provisioning - Reference Manual*.

MAP Policing (Manual Configuration of Maximum MAP Version)

The MAP Policing feature allows the operator to control, on a per-node and per AC basis, the maximum Application Context version to be used in any MAP transaction. This feature can be enabled or disabled in the system, as per the need of the operator.

With this feature enabled, the Tekelec ngHLR limits the MAP versions, during a MAP transaction, to the ones defined by the operator for each Application Context (custom AC templates) and per the Network Element (NE).

With the feature disabled, the custom AC templates are disregarded. The only template in use is the "Default Template", which contains the maximum values defined in the SS7 stack (GSM MAP Application Context).

This feature can be provisioned through the WebCI and CLI interfaces. The following needs to be provisioned by the operator:

- The enable/disable flag.
- A default maximum MAP version per Application Context (AC), which is a set of default values stored as a "Default Template", in the table "AC Template Definition".
- A maximum MAP version, per Application Context and per network element address range, for which the MAP Policing feature is applied only to Network Elements within that range. To do so, the template defined previously in the "AC Template Definition" table must be associated with a Node Range in the "AC Template Mapping" table. During a MAP transaction with a Network Element (NE), the Tekelec ngHLR limits the MAP versions to the values defined in the "AC Template

Mapping" table, if that NE is covered by a range defined in that table. Otherwise, if that NE is not covered by a range in the "AC Template Mapping" table, the Tekelec ngHLR limits the MAP versions to the values defined as the "Default Template" in the "AC Template Definition".

- During a MAP transaction, the Tekelec ngHLR proceeds with MAP Version Fallback when needed, and dynamically stores the last negotiated MAP version for a given AC, to be used for subsequent transactions. These values are stored in the "Node Number AC Mapping" table, dynamically managed by the Tekelec ngHLR. If a specific template is associated to the desired node, the values from this template are stored in this dynamic table; otherwise the values are taken from the "Default Template'.

The operator can restore the MAP versions stored in that dynamic table back to the original maximum values, which were defined as a template in the "AC Template Definition" table.

The MAP Policing feature also allows the operator to block certain MAP transactions based on the node address and the AC, by setting the maximum MAP version to "NotSupported" in an AC Template. That template must then be associated to a Node Range that covers the desired node address.

For more details on these tables and their parameters, please refer to the "*MAP Policing"* section in the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision these tables and execute the restore operation, please refer to the "Setting restrictions on the version of MAP messages (MAP Policing) and on the SRI-ack, ATI-ack and PSI messages" section in the *SDM System Configuration - User Guide*.

Map Reset

The Tekelec ngHLR offers the MAP_RESET service, which allows the operator to send a MAP_RESET message to VLRs or SGSNs in order to inform them that a failure occurred. The MAP_RESET message indicates to the remote node that it should refresh all of the subscriber data previously received by the Tekelec ngHLR. The following are the enhancements that have been made with the MAP Reset feature:

- Optimization of the list of VLRs to which the Tekelec ngHLR sends a MAP reset. A mechanism has been implemented to keep a count of the number of subscribers registered on a given node. That count is incremented upon an Update Location, decremented upon a Cancel Location, and stored in the database. The RESET message is sent only to the nodes that have registered subscribers (count > 0).
- Added capability to send MAP reset to only one GT, entered by the operator, using CLI or WebCI.
- Added capability to send MAP reset to a list of GT, imported by the operator, using CLI or WebCI.

With this feature, the operator can execute, from the CLI and WebCI, the SendMapReset() operation and choose to send MAP_RESET messages to all nodes, to only one node by specifying its Node Number and the HLR Number, and finally to a list of nodes imported from the NodeNumberSubset entity. Through the CLI and WebCI, the operator can define in the new NodeNumberSubset entity a specific list of nodes and their number. Moreover, to add facility to provision this NodeNumberSubset table, a new ManageNodeNumberSubset() operation has been implemented to clear that table or import all the nodes from the complete list of nodes stored in the database.

For more information on the SendMapReset() and ManageNodeNumberSubset() operations, refer to the "*MAP Policing Operations"* section in the *SDM System Configuration - Reference Manual*.

For more information about the NodeNumberSubset entity and its parameters, refer to the "MAP Policing" section in the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision the NodeNumberSubset entity through the WebCI, refer to the "MAP Reset" section of the *SDM System Configuration - User Guide*.

Active Location Retrieval

This feature allows the gsmSCF to retrieve the latest location of a subscriber, as stored in the VLR during the most recent location update procedure.

Active Location Retrieval (also known as current location retrieval) is an enhancement to MAP Any Time Interrogations (ATI) messages. With MAP ATI messages, the gsmSCF may obtain the subscriber's location information as currently stored in the VLR. The information in the VLR is stored during the most recent update location procedure. The location update procedure may be due to the subscriber changing location to another location area, call establishment or periodic location update.

With the ALR feature, the gsmSCF may instruct the VLR to page the subscriber, in which case the location information in the VLR will be refreshed and will then include the current cell id of the subscriber.

The following parameters, used to characterize the location of the subscriber, are supported in the MAP operations by the Tekelec ngHLR:

- Age of location
- Geographical Information
- VLR Number
- Location Number

The Tekelec ngHLR simply takes on the role of extracting the information from the ATI message received from the gsmSCF, and encapsulating it into a PSI message, destined to the VLR. The same mechanism is used for the PSI_response to the ATI

The ATI message contains a field (Current Location) that must be set to 1 in order to request a subscriber's active location. In the response message, the location information (Age of location, Geographical Information, VLR Number, Location Number) will be present or not, depending on the value of that field.

When an ALR is requested while the subscriber is in radio contact with the MSC/VLR (e.g. during a call), the MSC will not perform paging. However, the stored location in VLR is in that case already the current location. If the subscriber is detached from the MSC, then no paging will take place either.

This enhancement of the location update process is syntactically backwards compatible. The MAP operation versions used for the active location retrieval procedure are the same as for the regular location retrieval procedure. If the VLR does not support the transport of these parameters in the respective MAP operations, then the MAP respective operations are processed as for regular location retrieval procedure. That implies that the location retrieval succeeds, but without paging. The gsmSCF obtains the information stored in the VLR, but deduces from the absence of "*current location retrieved*" that the subscriber was not paged.

Optional PSI

As per 3GPP standards, when receiving an ATI or SRI message requesting a PSI message back, the Tekelec ngHLR returns a PSI message to the VLR or SGSN. However, the implementation of this feature allows the operator to choose to overrule this by blocking the PSI message a subset of Application Servers, even if it is requested in the SRI or ATI messages.

To achieve this, the PsiMsgOn parameter has been added to the AcTemplate entity within the Map Policing functionality. The operator can choose to block or not the PSI request from a node or node range (AS) by setting the PsiMsgOn parameter to '0' (PSI request blocked) or '1' (PSI request not

blocked) for a template, which can be in turn associated to a node or node range (originating node) through the AcTemplateMapping entity.

When the Tekelec ngHLR is provisioned with a PsiMsgOn set to '0' for a specific node or node range, this means that the Tekelec ngHLR blocks the PSI request sent in the ATI or SRI message from that specific node and doesn't send a PSI message.

When the Tekelec ngHLR is provisioned with a PsiMsgOn set to '1' for a specific node or node range, this means that the Tekelec ngHLR doesn't block the PSI request sent in the ATI or SRI message from that specific node and proceeds as per the standard by sending the PSI message to the VLR or SGSN.

Note: The action of enabling or disabling the MAP Policing feature dynamically has an impact on the Optional PSI feature. If the MAP Policing feature is disabled, then the PSI request is automatically enabled, and no PSI message is blocked if requested.

For more details on the PsiMsgOn parameter, refer to the "Map Policing" section of the *SDM System Configuration-Reference Manual*.

For instructions on how to configure an Application Context Template with the PsiMsgOn settings, refer to the "Setting restrictions on the version of MAP messages (Map Policing)" section of the *SDM System Configuration-User Guide*.

Subscriber Enable/Disable function

The "Subscriber Enable/Disable function" feature has been implemented to allow operators to determine if a given subscriber profile should be enabled or disabled. This feature allows the operators to minimize fraud, while improving the operability of the Tekelec ngHLR.

From a HLR MAP point of view, a disabled subscriber profile is treated as an inexistent subscriber. This means that all messages received for a subscriber with a subscriber profile configured as disabled are rejected.

With the implementation of this feature, the Tekelec ngHLR behaves as follows:

- When the operator provisions the subscriber profile to "ENABLE", the subscriber becomes enabled and hence visible to normal traffic.
- When the operator provisions the subscriber profile to "DISABLE", the subscriber becomes disabled and a Cancel Location is sent if the subscriber was registered.
- When a request arrives for a subscriber that is disabled, the Tekelec ngHLR responds with a NACK with "unknownSubscriber".
- When a request arrives for a subscriber that is enabled, the Tekelec ngHLR treats the request normally.

A flag "SubscriberState" has been implemented to allow the operator to enable/disable the subscriber. This flag is part of the configuration parameters when provisioning a subscriber profile (Primary IMSI). By default, at creation of a new subscriber profile, this flag is set to "ENABLE". Note that services can be added/removed for a subscriber independently of its state (set to "ENABLE" or "DISABLE"). The subscriber profile of a disabled subscriber can still be modified by a provisioning system.

At any time, the value of this flag can be changed manually by the operator through the WebCI or CLI. To do so, the operator must provision the following:

The "SubscriberState" parameter in the HLR application's SubscriberProfile entity.

In addition, a counter (Number_of_RequestToDisabledSubscriber) has been implemented in order to know the number of times a traffic request is refused because the intended subscriber is disabled.

For more details on the "SubscribeState" parameter implemented with this feature, refer to the "Subscriber Profile (Bearer Services, Teleservices, Called Barring, PreferredRoutingNetworkDomain)" section in the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision the Enable/Disable flag in a subscriber profile, refer to the "Viewing/Editing a HLR Service Profile" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Support of Access Restriction Data

The "Access Restriction Data" is a parameter in the ISD message that refers to the radio access technologies that are possibly restricted to a subscriber via subscription data.

In order to be compliant with VLRs/SGSNs that support the Access Restriction Data parameter, the Tekelec ngHLR now always sends to the VLR/SGSN the Access Restriction Data parameter in the ISD message during location update or restoration and includes it during Tekelec ngHLR initiated ISD messages only if the contents have changed. By default, the Tekelec ngHLR sends to the VLR a ISD message with an ARD parameter with the 0 (00000000) value. This means that, by default, the subscriber doesn't have any access restrictions.

Refer to the following 3GPP standards for more information on the "Access Restriction Data" MAP v.6 parameter: TS 29.002, TS 23.012, TS 23.008, TS 23.016, TS 23.211.

The AccessRestrictionData entity has been implemented in the Tekelec ngHLR to allow the operator to provision subscriber profiles with access restrictions, either from the WebCI, CLI or SOAP interface.

Provisioning the AccessRestrictionData entity of a subscriber profile defines access restrictions for that subscriber and prevents the VLR/SGSN/MME from assuming that the subscriber's profile doesn't have any restrictions enabled.

Note: If needed, this feature can be disabled by setting the AccessRestrictionData parameter to '1' in the HlrConfig entity.

For information on the HlrConfig entity's AccessRestrictionData parameter, refer to the "HLR Configuration" section in the *SDM System Configuration - Reference Manual*.

For more information on the AccessRestrictedData and the parameters to provision, refer to the *"Access Restriction Data"* section of the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision this entity, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

MAP SRI interworking with SIP subscribers

This feature has been implemented to enhance the call continuation for subscribers with both a GSM and SIP profile.

With this feature, a subscriber (with both GSM/SIP profile) can receive a call in the SIP domain (if SIP reachable), in the case where it appears to be unreachable in the GSM domain.

To achieve this, the Tekelec ngHLR's behavior has been enhanced to:

- Identify the cases where a call should be routed to SIP by verifying the status of the subscriber in both the GSM and SIP domains. After this verification, the Tekelec ngHLR behaves as follows:
    - If the subscriber is reachable in both the GSM and SIP domains: the Tekelec ngHLR verifies which one of these domains is provisioned as the preferred one and sends a PSI in the case where it is the GSM domain, otherwise it sends back a SRI-ack with the state/location reflecting the SIP Subscriber information.

  - If the subscriber is reachable only in the GSM domain: the Tekelec ngHLR sends a PSI to the VLR.
  - If the subscriber is reachable only in the SIP domain: the Tekelec ngHLR sends back a SRI-ack with the state/location as per provisioned in the HlrSipSubscriberInfo entity, implemented with this feature.

- Ensure that the SubscriberInfo parameters (state/location information) in the SRI-ack or ATI-ack messages are set to reflect a state and location that will allow a call to continue. By sending back, for a subscriber only reachable in the SIP domain, a SRI-ack with the state/location as per provisioned in the HlrSipSubscriberInfo entity, this allows the call to continue and to be routed to the SIP domain.

With this feature, the HlrSipSubscriberInfo entity has been implemented and from the WebCI, the operator can display it and edit the location, state and the non reachable reason (if applicable) defined for each HlrNumberConfig (Hlr addresses).

For more information on the HlrSipSubscriberInfo entity and the parameters to provision, refer to the "MAP SRI Interworking with SIP Subscribers" section in the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision this entity, refer to the "Configuring the MAP SRI Interworking with SIP Subscribers" section of the *SDM System Configuration - User Guide.*

Automatic device detection

This feature enables the Tekelec ngHLR to store the device model and software version used by the subscribers. This allows the operators to leverage this information for either marketing purposes, troubleshooting purposes, or simply for data mining/analytics purposes. The IMEI provides the unique identity of the device, and the SV provides the software/OS version.

In the case where the VLR sends a MAP Update Location or GPRS Update Location message with the IMEI-SV field populated, the Tekelec ngHLR now stores the following in the subscriber profile:

- The current and last IMEI-SV
- The timestamp of the last change of IMEI-SV
- The timestamp of the last time a VLR/SGSN reported the IMEI, regardless of whether it changed or not (last-report-timestamp)

After storing the ADD information, the Tekelec ngHLR then sends back an ISD message, as per the usual.

However, in the case where the "SkipSubscriberData" field is present in the UpdateLocation message (UL), it means that the UL is only meant to update the IMEI-SV, and the Tekelec ngHLR doesn't send back an ISD, but simply an Update Location-ack or Gprs UL-ack, as per the TS 29.002.

The operator can do the following from the WebCI:

- Enable/Disable the Automatic device detection feature by provisioning the ActiveDeviceDetection flag implemented in the HlrConfig table. This flag is dynamically configurable and set to OFF (disabled) by default. When turned OFF, the Tekelec ngHLR doesn't store the IMEI-SV information.
- View the stored Automatic device detection information for a subscriber profile, by displaying the SubscriberProfile table. The following parameters have been added to provide the necessary information:
  - CurrImeiSv: this parameter displays the current value of the IMEI-SV
  - PrevImeiSv: this parameter displays the previous value of the IMEI-SV
  - CurrADDTimestamp: this parameter displays the timestamp for the current IMEI-SV

- LatestADDTimestamp: this parameter displays the timestamp for the last time a valid IMEI-SV was received.

With this feature, the following counter has also been implemented in the Tekelec ngHLR in order to count the number of times an IMEI-SV has been changed in any Subscriber Profile:

Number_of_IMEI_SV_UPDATE_IN_SUBS_PROFILE

Ericsson MML Provisioning commands

With this feature, a MML protocol adaptor (MML-PA) has been implemented in order to handle the provisioning interface served by the Ericsson MML protocol. The Ericsson MML is a telnet based text protocol that requires a TCP server connection. It is capable of handling the Ericsson MML protocol and converts each MML command into Tekelec provisioning requests. Moreover, the MML-PA can serve multiple provisioning clients that use the Ericsson MML protocol in order to do provisioning.

T-CSI Suppression

The T-CSI Suppression feature has been implemented to allow the operator to inhibit the T-CSI information in the SRI message in the following conditions:

- The subscriber is roaming outside the HPLMN. This provides the operator the capability to control for which subscriber the T-CSI information can or cannot be sent out to the GMSC based on the subscriber's location.
- The subscriber is not reachable
- Call Forward (CFNRc, CFU) is detected for the subscriber.

The following has been implemented for this feature:

- The CSI Inhibition flag in the CamelCsiData entity, which allows the operator to set, for a specific subscriber, the T-CSI to the following options:
  - "CSI always sent" (default)
  - "CSI not sent in HPLMN"
  - "Don't send CSI when Not Reachable/CF or in HPLMN"
  - "Don't send CSI when Not Reachable/CF"

Note: This flag can only be set for the T-CSI.

When the CSI Inhibition flag is set to "CSI not sent in HPLMN" for a subscriber, the Tekelec ngHLR verifies if the PLMN in which the subscriber is located is defined as a Home PLMN in the HPLMN entity (entity provisionable by the operator, refer to "Support for multiple CC-NDC as Home PLMN" section). If it is the case, the Tekelec ngHLR then proceeds with the SRI call flow as if the subscriber has T-CSI "NOT provisioned".

When the CSI Inhibition flag is set to "Don't send CSI when Not Reachable/CF or in HPLMN" for a subscriber, the Tekelec ngHLR verifies all three conditions (subscriber not reachable, Call Forward detected, subscriber roaming in HPLMN) and if at least one condition is met, the Tekelec ngHLR proceeds with the SRI call flow as if the subscriber has T-CSI "NOT provisioned".

When the CSI Inhibition flag is set to "Don't send CSI when Not Reachable/CF" for a subscriber, the Tekelec ngHLR verifies all two conditions (subscriber not reachable, Call Forward detected) and if at least one condition is met, the Tekelec ngHLR proceeds with the SRI call flow as if the subscriber has T-CSI "NOT provisioned".

For details on the CSI Inhibition flag, refer to the "Camel Services" section of the *SDM Subscriber Provisioning - Reference Manual*. For details on the HPLMN entity, refer to the "Define HLR identities, HPLMN definitions and IMSI ranges" section of the *SDM System Configuration - Reference Manual*. For instructions on how to provision this feature for subscribers in bulk using XML files, refer to the *SDM Subscriber Provisioning - User Guide*. For instructions on how to modify, from the WebCI, a subscriber's profile in order to provision the CSI Inhibition flag, refer to the "Viewing/Editing HLR Subscriber Services" section of the *SDM Monitoring, Maintenance, Troubleshooting - User Guide*.

HLR profile optimization

With this feature, the HLR data model has been reconfigured for the following main reasons:

- To remove some limitations in the design of the Multi-IMSI feature.
- To allow IMSI-swap/SIM-swap for subscribers with Multiple-IMSI SIM cards.
- To allow the capability to group together the various facets of the subscriber profiles into the same subscription by adding a top level subscriber with a distinct key.
- To make the data model for HLR subscribers compatible for subscribers with many profiles/SIMs.

Hereunder are the changes made to the HLR data model:

- A top level Subscription entity has been added and has the following unique key: SubscriptionID. The SubscriptionID defines the HLR subscriber and each SubscriptionID can have multiple SIM cards, multiple HLR profiles (HlrServiceProfileID) and multiple MSISDNs. One subscriber can have only one single SubscriptionID in the Tekelec ngHLR and this SubscriptionID can be associated to multiple SIM cards, multiple MSISDNs and in the current release, to one single HLR profile (in a future release, it will be possible to associate a SubscriptionID to multiple HLR profiles).
- The SubscriptionID key replaces the old Primary IMSI key in the Sim entity. A SIM card data entry can be provisioned with or without assigning it to a SubscriptionID.
- The SimImsiMap entity has been added to allow the operator to define one or multiple IMSIs for a SIM card and specify which IMSI is the Primary IMSI.
- The MSISDN entity has been added to replace the MobileStation entity. It allows the operator to define one or multiple MSISDNs for a SubscriptionID (subscriber).
- The MsIsdnImsiProfileAssociation entity has been added to replace the old Multi-IMSI entity (entity used in releases previous to the current one, to define the Primary IMSI/MSISDN and multiple Alternative IMSIs/MSISDNs). The MsIsdnImsiProfileAssociation entity allows the operator to associate the IMSIs defined in the SimImsiMap entity to the MSISDNs defined in the MSISDN entity for the same SubscriptionID. It allows the operator to define one HlrServiceProfileID, which identifies one or multiple IMSI/MSISDN couples for one SubscriptionID. With this logic it's easy to associate an IMSI with a profile and to modify this association. This allows the possibility to perform a SIM swap with Multi-IMSIs.
- The SubscriptionID and HlrServiceProfileID keys replace the old Primary IMSI key in all the HLR subscriber profile/service provisioning entities. The presence of this key breaks the direct relation between an IMSI and a subscriber profile. In the current release, an association to a SubscriptionID and an HlrServiceProfileID must be made when creating a subscriber profile. An IMSI is associated to a subscriber profile through the MsIsdnImsiProfileAssociation. This offers the possibility to modify the IMSI/SIM relation and therefore more easily perform an IMSI/SIM swap for any subscriber.
- The following new operations have been implemented:
  - AddSIM(): this allows the Network Operator to create a SimId entry by defining a SIM card's data and its IMSI(s).

- AssignSIM()/UnassignSIM(): these operations allow the Network Operator to respectively assign a subscriber (SubscriptionID) to a provisioned SIM card (SimId) and unassign a subscriber from a SIM card (SimId).
- DeleteHLRSubscriber(): this allows the Network Operator to clean up the entries provisioned in all the HLR entities specifically for a subscriber (SubscriptionID).
- ModifyDisplayedMSISDN(): this allows the Network Operator to

  change the displayed flag from one MSISDN to another MSISDN (same IMSI).

For more details on these operations and on each of the entities implemented with this feature, refer respectively to the "HLR Operations" and "HLR entities" sections of the *SDM Subscriber Provisioning - Reference Manual*. For instructions on how to provision SIM cards and/or HLR Subscribers in bulk, refer to the XML files in the *SDM Subscriber Provisioning - User Guide*. For instructions on how to view/modify from the WebCI a subscriber's profile, refer to the "Viewing/Editing HLR Subscriber Profile" section in the *SDM Monitoring, Maintenance, Troubleshooting - User Guide*.

Multi Imsi Enhanced feature

The Multiple Imsi feature has been implemented to support the use of Multi-IMSI SIM cards. This feature allows a HLR subscriber to be identified with multiple pairs of IMSI and MSISDN values, with one pair being the Primary pair used in the Home PLMN (Primary IMSI and MSISDN) and all the others being alternate pairs (Alternate IMSI and b MSISDN), which are used in Visited PLMNs.

With this feature, the following business solutions have been implemented in the Tekelec ngHLR:

- The "low-cost roaming" solution: multiple IMSIs with one single MSISDN
- The "virtual number" solution: one IMSI with several MSISDNs
- Any combinations of the above, i.e. "m" IMSIs with "n" MSISDNs

When entering a network, the subscriber is registered with the IMSI MSISDN pair that is the most cost efficient in the visiting network, thus reducing roaming service charges. However, the subscriber is reachable in the visiting network through all published MSISDNs provisioned in the HLR

Each IMSI/MSISDN pair assigned to the subscriber is programmed in the subscriber's SIM card and then provisioned by the subscriber's home network operator in the Home HLR. In the Tekelec ngHLR, the operator can provision a subscriber with Multiple IMSI/MSISDN pairs as follows:

SIM cards can be provisioned in the Sim entity and can be assigned or not to a subscriber by specifying the SubscriptionID.

The IMSIs programmed in the SIM card can be provisioned in the SimImsiMap entity for a specific SimId and the MSISDNs can be provisioned in the MSISDN entity for a specific SubscriptionID. In this entity, each MSISDN can be provisioned as 'published' or 'not published' with the Published flag in order to define whether or not the SRIs for a given MSISDN are accepted or rejected by the Tekelec ngHLR.

For a specific HlrServiceProfileID (identifier of a HLR subscriber profile), IMSIs and MSISDNs can be associated together in pairs and provisioned as a Primary or Alternate pair. Moreover, in this entity, each IMSI/MSISDN pair can be provisioned as 'displayed' or 'not displayed' with the Displayed flag in order to define whether the Alternate MSISDN can be transmitted or not in an ISD message.

- With the implementation of the ModifyDisplayedMSISDN() operation, the Network Operator can change the displayed flag from one MSISDN to another MSISDN (same IMSI) without needing to delete/re-create the Alternate IMSI/Alternate MSISDN entry from the MsIsdnImsiProfileAssociation.

The Tekelec ngHLR sends a Cancel Location message (GPRS and/or Non-GPRS) when:

- The last association of a registered IMSI is deleted from the MsIsdnImsiProfileAssociation entity.
- The association of a registered IMSI for which the Displayed flag is 1 is modified.

The Tekelec ngHLR now sends an ISD message with the new MSISDN when:

- The MSISDN , associated with an IMSI that is registered and that has the Displayed flag set to '1', is modified. This is the case, if the IMSI is not modified, but only the MSISDN.

For more details on the MsIsdnImsiProfileAssociation entity implemented to provision the Multi-IMSI feature, refer to the "MSISDN-IMSI Profile Association" section of the *SDM Subscriber Provisioning - Reference Manual*. For more details on the ModifyDisplayedMSISDN() operation, refer to the "HLR Operations" section of the *SDM Subscriber Provisioning - Reference Manual*.

For an example of a XML file that provisions a HLR subscriber with multiple MSISDN-IMSI couples (Multi-IMSI feature), refer to the "Examples of XML files for subscriber provisioning" chapter in the *SDM Subscriber Provisioning - User Guide*.

For instructions on how to view/modify from the WebCI the MSISDN-IMSI Profile Associations for a specific subscriber (SubscriptionID), refer to the "Viewing/Editing HLR Subscriber Profile" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Shared MSISDN across subscribers for Calling Line Identification

With the implementation of this feature, the Network Operator can:

- Associate multiple IMSIs of a subscription's different SIM cards with the same MSISDN. In other words, each mobile/SIM defined for a specific subscription (SubscriptionID) can share the same MSISDN.
- Associate multiple IMSIs of different SIM cards belonging to different subscriptions (SubscriptionID) with the same MSISDN. In other words, each mobile/SIM defined in different subscriptions can share the same MSISDN.

This allows all the mobiles/SIMs that use the same MSISDN (aka: shared MSISDN) to have the same Calling Line Identification (CLI). Only one mobile/SIM that uses a shared MSISDN is able to receive incoming calls but all the mobiles/SIMs that share an MSISDN are able to make outgoing calls.

This means that the Network Operator can/must perform the following from one of the available User Interfaces (CLI, WebCI, CommandFileLoader, SOAP/XML):

- Define a MSISDN as "shared" (when needed) by setting the 'Shared' flag to '1' in the MSISDN table, which means that it can be used by any mobile/SIM of any subscription (SubscriptionID).
- Define each MSISDN-IMSI profile association as "reachable" or "not reachable" by setting the 'Reachable' flag to '1'or '0' respectively. This allows the Network Operator to set which mobile/SIM can receive calls. This will indicate to the Tekelec ngHLR which MSISDN-IMSI profile association to choose between all the different associations that use the same MSISDN and therefore which SIM can be reached. For this logic to be followed correctly, the following rules must be respected by the Network Operator when provisioning the MSISDN-IMSI profile associations:
  - All the MSISDN-IMSI profile associations defined for one single SIM with the same MSISDN must all have the 'Reachable' flag set to the same value.
  - There must be one and only one reachable SIM among the ones that have MSISDN-IMSI associations that use the same shared MSISDN. A SIM is reachable if the MSISDN's 'Published' flag and the MSISDN-IMSI association's 'Reachable' flag are both set to '1' (true). By default, the 'Reachable' flag is set to '1'. For a MSISDN, if there is no 'Reachable' flag set to true ('Reachable=1') for one of its MSISDN-IMSI associations, all the MSISDN based messages will fail for this specific MSISDN.

To change the reachable flag of many IMSI-MSISDN associations of the same SIM, two new operations have been created: MakeMsisdnNotReachable () and MakeMsisdnReachable ().

By allowing MSISDN-IMSI associations with a shared MSISDN and by using the 'Displayed' flag on the shared MSISDN-IMSI association, in the update location procedure, all mobiles/SIMs with the same shared MSISDN will send ISD with the same MSISDN and use the same CLI.

Examples of a scenario with mobiles/SIMs using shared MSISDN

A group of three customer support representatives each has a different number to be reached at, but have the same number (for example a dispatcher office number) to be displayed to the customers when they are calling them for handling their support requests (see figure below). In this example, when the customer tries to reach the shared MSISDN "CC", only the Call Center mobile can be reached since it is the one with the MSISDN-IMSI association set to 'Reachable=1'.

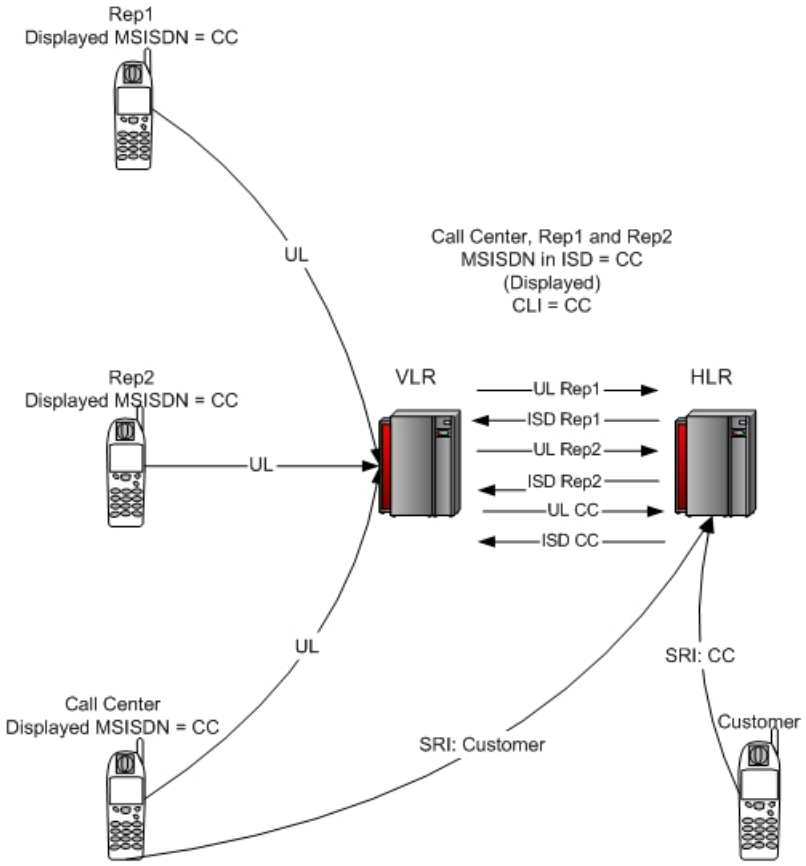


Figure 27: Example using Shared MSISDN across CLI

Here is what the database table should look like for this example:

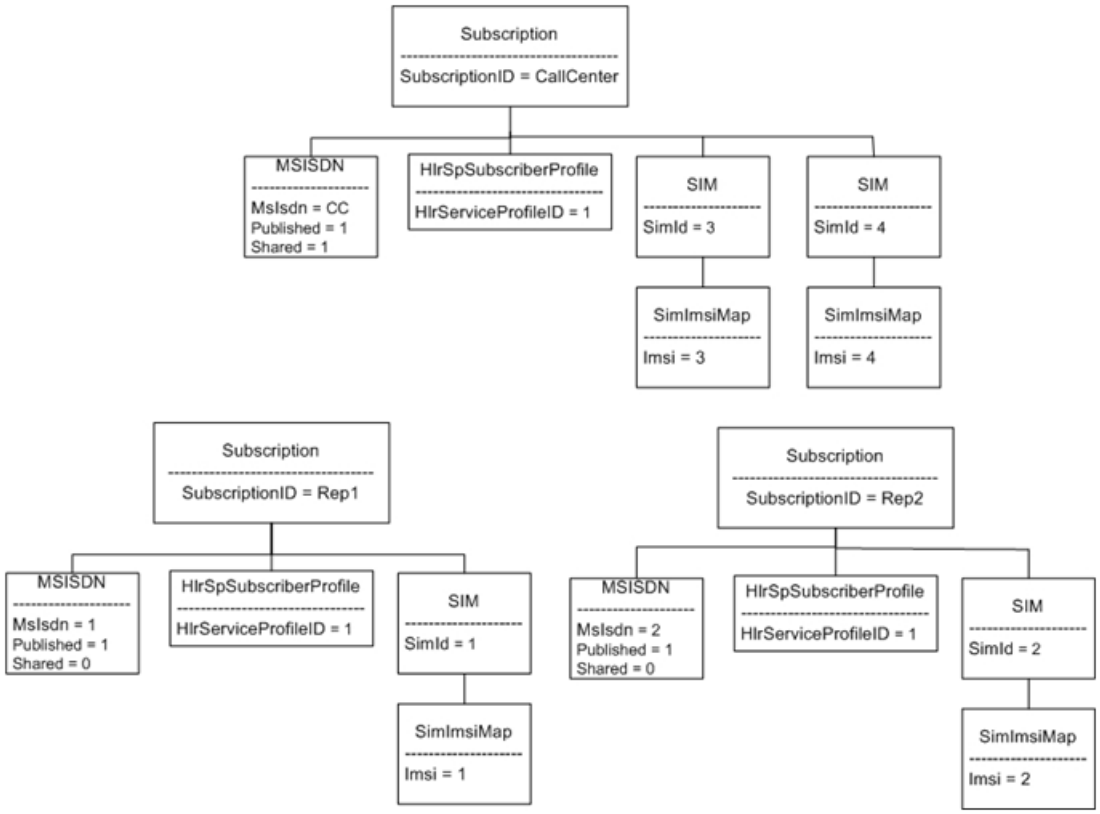


Figure 28: Shared MSISDN

Here is what the association table must look like for this example:

Table 20: MsIsdnImsiProfileAssociation table

SubscriptionID	HlrServiceProfileID	Imsi	MsIsdn	Displayed	Reachable
Rep1	1	1	CC	1	0
Rep1	1	1	1	0	0
Rep2	1	2	CC	1	0
Rep2	1	2	2	0	0
CallCenter	1	3	CC	1	0
CallCenter	1	4	CC	1	1

This allows Rep1, Rep2 and CallCenter (both SIM of Call Center) to send the same MSISDN in the Update Location message (Displayed MSISDN = CC for all the Subscribers). By setting the Reachable flag to 1 for Call Center SIM4/IMSI4, this means that all MSISDN based messages will go to the Call Center and use the volatile data of Sim4/IMSI4.

For a detailed description of the 'Shared' flag and of the 'Reachable' flag, refer to the "MSISDN" and "MSISDN-IMSI Profile Association" sections respectively in the *SDM Subscriber Provisioning - Reference Manual* . For details on how to execute the MakeMsisdnNotReachable () and MakeMsisdnReachable

() operations from the CLI, refer to the "HLR Operations" section of the *SDM Subscriber Provisioning-Reference Manual* document. If you wish to perform these operations from the WebCI, simply click on the corresponding buttons located below the MsisdnImsiProfileAssociation table (see 'Viewing/Editing SIM cards, MSISDNs, IMSIs and HLR Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting-User Guide document)*.

Enhanced SIM-swap/IMSI-swap

The enhanced SIM-swap/IMSI-swap feature allows the operator to change the SIM (with one or many IMSIs) of a subscriber to another SIM (with one or many IMSIs) that is unassigned (not linked to a SubscriptionID), while keeping the same MSISDN(s) and all the data of the subscriber provisioned as is in its profile (HLR Service Profile, MSISDN and association).

This feature is specifically useful in cases where a subscriber loses its SIM card, but wants to keep all its subscription information unchanged (MSISDN, etc.).

Moreover, the SimSwap counter has been implemented to count the number of times the SwapSIM() operation is executed.

The conditions under which the SwapSIM() operation can be executed are the following:

- The old and new SIM cards must exist in both the Sim and SimImsiMap entities.
- The new SIM must be unassigned, which means it must not be linked to any subscriber (SubscriptionID: 'null').
- The new IMSI(s) of the new SIM cards must not be provisioned in the MsIsdnImsiProfileAssociation table because the operation changes the IMSI, but do not overwrite an existing IMSI (association). In other words, the new SIM cards must not be already assigned.
    - The number of IMSIs for the new SIM card (provisioned in the SimImsiMap entity) must be greater or equal to the number of IMSIs provisioned in the MsIsdnImsiProfileAssociation entity for the old SIM card.

When the SwapSIM() operations is executed, the Tekelec ngHLR performs the following:

- Assigns a new SIM card to the subscriber (SubscriptionID), by unassigning the old SIM data and assigning the new SIM data to the subscriber.
- Sends a Cancel Location
- Deletes the volatile data for the old SIM Card
- Deletes all associations of the Old SIM Card (all Old IMSI).
- Increments the SimSwap counter.
- If the DeleteOldSIM option is set to '1' when executing the SIM-swap/IMSI-swap operation:
    - The Tekelec ngHLR deletes the old SIM data entry from the Sim entity and deletes all the IMSIs provisioned for the old SIM in the SimImsiMap entity.
- If the AutoMap option is set to '1' when executing the SIM-swap/IMSI-swap operation:
    - This option is recommended when swapping SIM cards that contain Multi-IMSIs. The Tekelec ngHLR changes all the old IMSIs defined in the MsIsdnImsiProfileAssociation entity with the new IMSIs by using a MCC/MNC best matching mechanism. This establishes new MSISDN-IMSI associations with IMSIs (MCC/MNC) that are as compatible as possible between the old and the new SIM card. The Multi-IMSIs of the new SIM card should have the same MCC/MNC as the old SIM card.

If this option is not chosen, the operator must provision manually the new IMSIs for the new SIM in the MsIsdnImsiProfileAssociation entity.

- If the Deferred option is set to '1' when executing the SIM-swap/IMSI-swap operation:
  - The complete SIM-swap operation will only be executed upon the first Update Location of one of the new SIM card's IMSIs.

A CancelDeferredSwap() operation has also been implemented to allow the Network Operator to cancel the deferred SIM-swap operation (SwapSIM() with Deferred= '1').

For more details on the SwapSIM() and CancelDeferredSwap() operations and on how to display the list of "pending" SIM-swap operations (SimSwapDeferred entity), refer to the *SDM Subscriber Provisioning - Reference Manual*'s "HLR Operations" and "SIM-swap Deferred" sections respectively.

For instructions on how to execute the SwapSIM() and CancelDeferredSwap() operations from the WebCI, refer to the *SDM System Configuration - User Guide*.

For more details on the SimSwap counter, refer to the *SDM Performance Measurements* document.

Subscriber Signaling Router (SSR)

With this feature, the basic functionality of a Subscriber Signaling Router (SSR) has been implemented in the Tekelec ngHLR. It provides the Network Operator the ability to configure the Tekelec ngHLR to redirect some SS7 messages to an alternate HLR address, using the following rules:

- Based on an individual IMSI or MSISDN number.
- Based on IMSI of MSISDN number range.
- Based on absence of subscriber.
- Based on message type (SAI/ATI override)

This is useful to maintain service to the end users while in the process of migrating HLR subscribers from a legacy HLR to a Tekelec ngHLR.

Only Open messages (TCAP begin) can be handled by the SSR, so only those messages are able to be forwarded. The Continue and Close messages are always handled locally. Moreover, when receiving a RegisterSS or EraseSS or ActSS or DeactSS message for a user that is not registered locally, the Tekelec ngHLR blocks the message.

In order to provide to the Network Operator the ability to configure the Tekelec ngHLR with the SSR functionality, the following attributes and entities have been added to the Tekelec ngHLR. Note that these attributes/entities can be provisioned through either one of the SDM interfaces (CLI, WebCI, XML).

- The SubscriberSignalingRouter attribute has been added to the HlrConfig entity in order to allow the Network Operator to view dynamically the SSR activation state. If the Tekelec *Customer Care Center* has authorized the SSR activation, the Network Operator can activate or deactivate the feature by executing the ActivateFeature() or DeactivateFeature() operations.
- The HlrSSRPerSubData entity has been added to allow the Network Operator to assign a SSR Template definition to a subscriber.

The HlrSSRPerIMSIRangeData entity has been added to allow the Network Operator to assign a SSR Template definition to a specific IMSI or an IMSI range (IMSI Prefix in E.212).

- The HlrSSRPerMSISDNRangeData entity has been added to allow the Network Operator to assign a SSR Template definition to a specific MSISDN or an MSISDN range (MSISDN Prefix in E.164).

- The HlrSSRTemplate entity has been added to allow the Network Operator to define SSR templates with the following SSR data:
  - SSR template description
  - Forwarding address (E.164 number)
  - TimeStamp
  - Block user changes (Never/Always/Before_UL/After_UL)
  - Forward messages (Never/Always/Before_UL/After_UL)
  - Forward SAI override (bool=no/yes)
  - Forward ATI override (bool=no/yes)

The following additional operations have been implemented and can only be executed from the CLI:

- DisplaySSRVolatileData(): this operation can be executed to display the SSR Volatile data of a specific subscriber.
- DisplaySSRStatistic(): this operation can be executed to get the number of 'first Update Location' received and to print into the traces the counters' values.
- UpdateTimeStamp(): this operation can be executed to refresh the HlrSSRTemplate entity's TimeStamp to the current time.

When receiving an Open message, the Tekelec ngHLR now verifies if the SSR functionality is active in order to know if the message must be processed locally or not. The message is processed locally as usual if the SSR is not active.

On the other hand, in the case where the SSR functionality is active, the Tekelec ngHLR verifies the following in this order:

1. If the subscriber is provisioned in the Tekelec ngHLR's database:
   a. If the subscriber match one of "Per-subscriber SSR data", process this template
   b. If the subscriber does not match one of "Per-subscriber SSR data", process this message locally
2. If the incoming IMSI matches one of the "Per-IMSI range SSR data", process this template
3. If the incoming MSISDN matches one of the "Per-MSISDN range SSR data", process this template

Note: For the SSR range data (HlrSSRPerMSISDNRangeData and HlrSSRPerIMSIRangeDate), a common BestMatch algorithm is used to extract the range that best matches the incoming IMSI or MSISDN number.

If the incoming message matches one of the SSR data (1a, 2 or 3), then the appropriate SSR template provisioned in the HlrSSRTemplate entity is extracted and investigated as follows to take the appropriate message processing action:

- If the Incoming message is a Register/Erase type, and if the following request to block:
- If the BlockUserChange attribute is set to 'Never', then the Tekelec ngHLR never block the message (continue to 2)
- If the BlockUserChange attribute is set to 'Always', then the Tekelec ngHLR blocks the message (silently discarding it)
- If the BlockUserChange attribute is set to 'Before_UL', then the Tekelec ngHLR blocks (silently discarding it) the message until an Update Location is received for the user, all subsequent messages (including UL) will not be block (continue to 2)
- If the BlockUserChange attribute is set to 'After _UL', then the Tekelec ngHLR does not block (continue to 2) until an Update Location is received for the user, all subsequent messages (including UL) are blocked (silently discarding it).

- If the incoming message is an SAI, and if the Forward SAI Override is 'ON' (1), then the Tekelec ngHLR forwards the message.
- If the incoming message is an ATI, and if the Forward ATI Override is 'ON' (1), then the Tekelec ngHLR forwards the message.
- The template Forwarding selection will be processed:
- the Forward attribute is set to 'Never', then the Tekelec ngHLR will process this message locally.
- If the Forward attribute is set to 'Always', then the Tekelec ngHLR will forward the message to the configure address
- If the Forward attribute is set to 'Before_UL', then the Tekelec ngHLR forward the message to the configure address until an Update Location is received for the user, all subsequent messages (including UL) will be processed locally.
- If the Forward attribute is set to 'After _UL', then the Tekelec ngHLR process locally until an Update Location is received for the user, all subsequent messages (including UL) are forwarded to the configure address.

Forward messages are for all MAP messages (the Begin message) and block user changes applies for RegisterSS, EraseSS, ActSSg, DeactSS messages.

For more details on the new attributes/entities implemented with this feature, refer to the "Subscriber Signaling Router" section of the *SDM System Configuration - Reference Manual*. For more details on the operations implemented with this feature, refer to the "HLR Operations" section of the *SDM System Configuration - Reference Manual*.

For instructions on how to provision this feature through the WebCI, refer to the "Provisioning the Subscriber Signaling Router (SSR)" section in the *SDM System Configuration - User Guide*.

Dual-SIM priority calling

The "Dual-SIM priority calling" feature allows a Tekelec ngHLR subscriber to have two devices (two different SIM cards) registered simultaneously and if the first SIM cannot be reached for any CFNRc scenario (example: absent subscriber), the Tekelec ngHLR automatically tries to reach the subscriber's second device (SIM) by setting the MSISDN of the second SIM as a Forward-to-Number in the SRI-ACK message. To achieve this, a new concept of Priority has been implemented between a subscriber's MSISDNs.

By default, all of a subscriber's MSISDNs have the Priority set to '0', which means that this feature is disabled. In order to enable this feature for a subscriber, the SIMs of its two devices must both be provisioned under the same SubscriptionID with a unique IMSI for each. For one of these two SIMs, one of its provisioned IMSI-MSISDN couple must have a Priority set to '1' and for the other one of the two SIMs, one of its provisioned IMSI-MSISDN couple must have a Priority set to '2'.

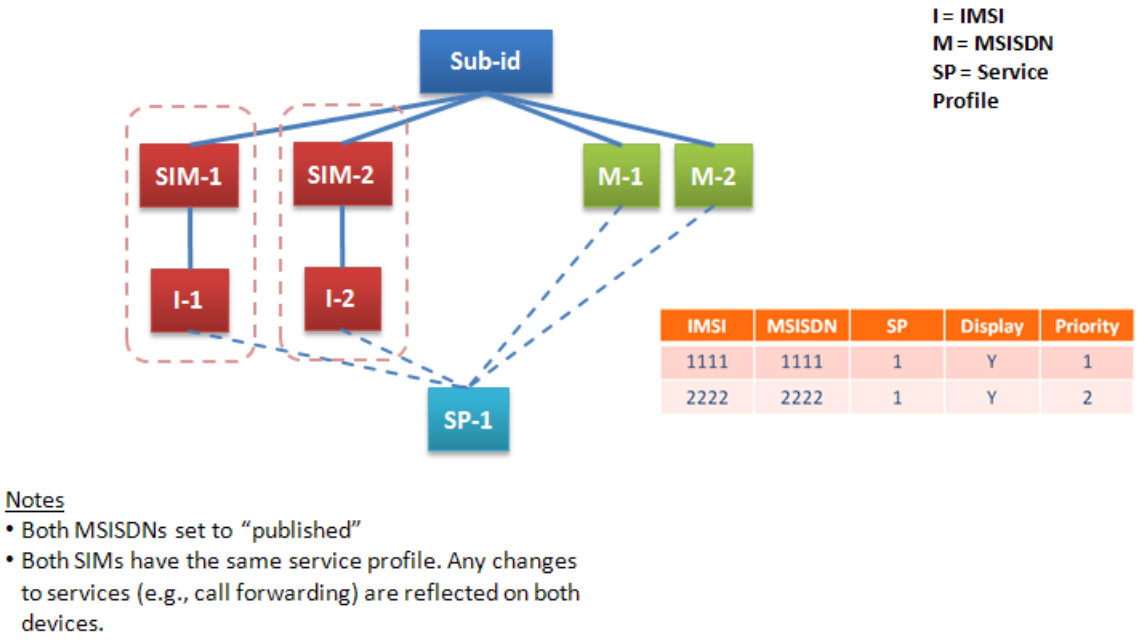


Figure 29: Dual-SIM Priority Calling

If the MSISDN with Priority '1' on SIM 1 cannot be reached for any CFNRc scenario, the Tekelec ngHLR automatically sends the MSISDN with Priority '2' of the SIM 2 as the ForwardToNumber in the SRI-ack. This allows the call to be redirected to the SIM for which the MSISDN is set to Priority '2'.

In order to provide to the Network Operator the ability to provision the Dual-SIM priority calling feature for a subscriber, the new "Priority" attribute has been added to the MsIsdnImsiProfileAssociation entity.

For details on the MsIsdnImsiProfileAssociation entity's Priority attribute, refer to the "MSISDN-IMSI Profile Association" section of the *SDM Subscriber Provisioning - Reference Manual*.

VLR link congestion handling

With this feature, the traffic congestion control functionality has been added to the Tekelec ngHLR. It allows the Network Operator to be able to manually reduce the SS7 traffic by controlling, until the VLR recovers from an overload condition, the quantity of PRN and ISD messages sent towards the HPLMN VLRs.

To achieve this, the following three new operations have been added from the HLR entity and can be executed by the Network Operator from the CLI in order to enable/disable this feature:

VlrRecoveryModeEnable()IsdCompressed_percent =*percent1*; PrnSupressed_percent =*percent2*

Where:

- *Percent1*: integer from 0-100. Specifies the percentage of the UL that will trigger ISD uploading minimal subscriber profile to the HPLMN VLR.
- *Percent2*: integer from 0-100. Specifies the percentage of PRNs toward the HPLMN VLR that will be suppressed (not sent).

Note: If the ISD_compressed% is > 0 and/or the PRN_suppressed% is > 0 the feature is considered enabled. The feature is considered disabled if both ISD compression and PRN suppression parameters are set to 0%.

When the VlrRecoveryMode is enabled with parameter IsdCompressed_percent parameter > 0 and <=100, a certain amount of ULs will trigger ISDs that upload minimal subscriber profile that will be contained in a single ISD.

The definition of a minimal (compressed) Subscriber Profile is the following:

- Imsi
- MSISDN
- TS11 TS21, TS22, if provisioned in the subscriber profile
- BOIC for speech, regardless of whether it is provisioned in the subscriber profile
- CLIR as provisioned in the subscriber profile

When the VlrRecoveryMode is enabled with parameter PRNsupressed_percent parameter > 0 and <=100, a certain amount of the PRNs that are to be sent to the HPLMN VLR are not sent. Instead, the SRI processing continues as if a PRN has been sent and PRN Rasp with error `RoamingNotAvailable` has been received. This results in SRI Ack with the SIPNumber, CFNumber with/without Camel info, depending on the subscriber's profile and registration.

Note: The PRN suppress mode does not have control over the PSIs triggered. Even if PRNsupressed_percent = 100%, PSIs are still sent to the HPLMN VLR.

The table below presents the number of PRN suppressed/sent or the number of ISD compressed/full for each percentage set for either the PRNsupressed_percent parameter or for the IsdCompressed_percent parameter.

Table 21: PRN compression

% PRN suppressed (% ISD compressed)	PRN suppressed/sent (or ISD compressed/full)
100% 96%	All PRN Suppressed (ISDs compressed)
95%	1 of 20 PRN sent
94%	1of 16 PRN sent
93%	1 of 14 PRN sent
92%	1 of 12 PRN sent
91%	1 of 11 PRN sent
90%	1 of 10 PRN sent
89%	1 of 9 PRN sent
88%	1 of 8 PRN sent
87 % 86%	1 of 7 PRN sent
85% 84%	1 of 6 PRN sent
83% 80%	1 of 5 PRN sent
79% 75%	1 of 4 PRN sent

74% 67 %	1 of 3 PRN sent
66% 51%	1 of 2 PRN sent
50% 34%	1 of 2 PRN suppressed
33% 26%	1 of 3 PRN suppressed
25% 21%	1 of 4 PRN suppressed
20% 17%	1 of 5 PRN suppressed
16% 15%	1 of 6 PRN suppressed
14% 13%	1 of 7 PRN suppressed
12%	1 of 8 PRN suppressed
11%	1 of 9 PRN suppressed
10 %	1 of 10 PRN suppressed
9 %	1 of 11 PRN suppressed
8%	1 of 12 PRN suppressed
7%	1 of 14 PRN suppressed
6%	1 of 16 PRN suppressed
5%	1 of 20 PRN suppressed
4% 0%	0 suppressed

- VlrRecoveryModeDisable():

  This operation allows the Network Operator to disable this feature. This operation will set both the IsdCompressed_percent and PRNsupressed_percent parameters to 0%.

- VlrRecoveryModeGet():

  This operation allows the Network Operator to display the IsdCompressed_percent and PRNsupressed_percent parameters.

In addition to these operations, the following new alarms with severity "Warning" have been implemented:

AlarmId: `9138`> VlrRecoveryMode has been deactivated. This alarm is raised every time the feature goes from Enabled to Disabled.

AlarmId: `9137`> VlrRecoveryMode [Isd Compressed =*x*% Prn Suppress =*y*%] has been activated. Where x and y is a number within a 0-100 range. This alarm is raised every time the feature goes from Disabled to Enabled and every time the IsdCompressed_percent/PrnSuppressed_percent parameters are modified.

For more details on these operations, refer to the "HLR Operations" section in the *SDM System Configuration - Reference Manual*.

For more details on the alarms implemented in this feature, refer to the *SDM Alarm Dictionary*.

ISD failed flag

In order to provide an indication to the Network Operator of whether or not the changes made to an Tekelec ngHLR's subscriber data from an external provisioning system have been successfully propagated to the VLR, an ISD Failed flag has been added to the series of VLR flags in the HLR volatile data. With this new feature, the Network Operator can now view the ISD status by displaying the HlrVolatileData entity for a subscriber.

The Tekelec ngHLR sets the ISD Failed flag to 'ISDFailed' under the following conditions:

- If an ISD message initiated by the Tekelec ngHLR has failed and a NACK response has been received.
- If one of the ISD messages sent by the Tekelec ngHLR in response to an Update Location request has failed.

The ngHLR resets the ISD Failed flag and removes the 'ISDFailed' value under the following conditions:

- If an ISD message initiated by the Tekelec ngHLR has passed and an ACK response has been received.
- If all of the ISD messages sent by the Tekelec ngHLR in response to an Update Location or Update Location GPRS request have passed.
- If a Cancel Location is successful.

For more details on the ISD Failed flag, refer to the 'VlrFlags' parameter in the HlrVolatileData entity in the "HLR Volatile Data" section of the *SDM Subscriber Provisioning - Reference Manual*.

Per Subscriber ATI screening

The Tekelec ngHLR goes through a series of rules when processing and analyzing the ATI message received in order to determine what messages (PSI and/or ATI-ack) to send in response to the request and what to include in them based on what is requested in the ATI message and on what is provisioned in the Tekelec ngHLR's database for the originating node or node range. Now, with the implementation of this feature, additional sets of rules have been implemented to the already existing ones in the ATI Request process and in the PSI and ATI-ack message building processes. These additional rules allow the Network Operator to control, on a per subscriber basis, whether the PSI message is suppressed or not and how much information can be included in the ATI-ack messages.

The sets of rules implemented with this feature offer an additional ATI screening based on the level of information provisioned by the Network Operator for each subscriber. The different possible levels of information are as follows:

- Send no location/state info
- Send inside/outside HPLMN indication, plus subscriber state held at HLR
- Send HLR-stored location/state (i.e. VLR number and state retrieved from HLR volatile data)
- Send VLR-stored location/state (i.e. PSI sent without ALR, location/state retrieved from PSI-rsp)
- Send complete VLR location/state (i.e. normal processing path)

Note: The following:

- **Settings a, b and c suppress the PSI message**
- **Setting d allows the PSI message but suppresses the ALR parameter (currLoc)**

- **Setting b returns a location in the form of a pre-configured node number, based on the current location of the subscriber (inside or outside of HPLMN). If the location is unknown, the location field will be left empty.**

To achieve this, the AtiSubsInfoLevel parameter has been added to the database's SubscriberProfile entity to allow the Network Operator to set one of the above settings for a specific subscriber profile. Moreover, the 'InsideHplmnIndication' and 'OutsideHplmnIndication' parameters have been added to the HPLMN entity to allow the Network Operator to define some generic node numbers when a subscriber is located inside its Home PLMN, or outside of its Home PLMN. These values are used to set the subscriber location in the ATI-ack when option b is selected. The fields can be left empty, in which case no location information will be sent in the ATI-ack.

For more information on the AtiSubsInfoLevel parameter and its possible values, refer to the SubscriberProfile entity in the *SDM Subscriber Provisioning - Reference Manual*. To know how to edit it from the WebCI, refer to the "Viewing/Editing HLR Subscriber Profile" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide.*

For more information on the parameters added to the HPLMN entity, refer to the "Define HLR identities, HPLMN Definitions and IMSI ranges" section in the *SDM System Configuration - Reference Manual*. For instructions on the provisioning of these parameters from the WebCI, refer to the "Defining PLMNs, multiple Home PLMNs and HPLMN Countries" section of the *SDM System Configuration - User Guide*.

Call Forward re-activation with RegisterSS

As per the 3GPP standards, after deactivating a Call Forward service with DeactivateSS, it cannot be re-activated directly with a RegisterSS. The CF must be de-registered first with EraseSS and only then will a RegisterSS register and activate the CF. As another option, the CF can be re-activated simply with ActivateSS. However, certain mobile stations don't follow the standards and try to re-activate the CF directly with a RegisterSS.

In order to accommodate these mobile stations, the Tekelec ngHLR allows the CF services to be re-activated with RegisterSS without having to de-register it first with EraseSS.

The DirectCallForwardRegistration parameter has been added to the HlrConfig entity in order to allow the Network Operator to enable/disable this feature. By default it is disabled and the CF re-activation process follows the 3GPP standards. For more details on this parameter, refer to the "HLR Configuration" section of the *SDM System Configuration - Reference Manual*. For instructions on how to modify this parameter and activate this feature, refer to the "Viewing activation status of HLR features and activating/deactivating them individually" section of the *SDM System Configuration - User Guide*.

OP (Operator Variant) per subscriber

The Network Operator can choose to provision an OP (Operator Variant) for either one of the following:

- For each algorithm. This means that the same OP is used for all SIMs referring to the same algorithm.
- For each SIM card. This means that each SIM card can be provisioned with its own OP (Operator Variant) instead of using the global OP of the Algorithm. Each subscriber (SubscriptionID) can have multiple SIM cards provisioned and each can have a different OP.

The OP is used for the SAI (Send Authentication Info) message, it indicates whether the Tekelec ngHLR must generate Triplets or Quintuplets if the Algorithm is GSM Milenage or UMTS Milenage. The OP is only used in the cases where authentication must be done using the GSM Milenage or UMTS Milenage algorithm.

Note: The OP provisioned for the SIM overwrites the global OP provisioned for the algorithm. In the case where no OP is provisioned for the SIM, the global OP provisioned for the algorithm is used when necessary.

With the implementation of the OP per subscriber feature, the "Op32HexChar" attribute has been added to the SIM entity. The Network Operator can therefore define an OP when provisioning a SIM card, by provisioning the SIM entity's "Op32HexChar" attribute with the desired OP value.

The provisioning of the SIM card can be achieved with XML Templates (refer to the *SDM Subscriber Provisioning - User Guide*) or through the WebCI (refer to the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*). For details on the "Op32HexChar" attribute and the supported value range, refer to the *SDM Subscriber Provisioning - Reference Manual*.

Enhanced Control of SCCP Routing

Note: The "Enhanced Control of SCCP Routing" feature is optional and must be purchased from Tekelec to be available. If this feature has been purchased, then this description details how SCCP routing is conducted when either the feature is deactivated (default setting) or is activated.

At system start-up, the "Enhanced Control Of SCCP Routing", and the "Update of SCCP Calling Address only for Update Location" features can be dynamically activated/deactivated by the Network Operator during running time of the system by executing the HlrConfig's ActivateFeature() and DeactivateFeature() operations and specifying these features.

Note: The "Update of SCCP Calling Address only for Update Location" should be deactivated in order for the "Enhanced Control of SCCP Routing" feature to work properly for all MAP messages.

The Enhanced Control of SCCP Routing feature has been implemented to always return the correct HLR Number as the Calling address in the supported MAP messages. The ngHLR analyses the received SCCP called party address to determine the correct HLR Number that is returned in the MAP response's SCCP calling party address.

The Network Operator can control the activation of this feature for:

- All MAP messages, except for the FUNCTIONAL_SS_CONTEXT and NETWORK_UNSTRUCTURED_SS_CONTEXT.
- Only the Update Location and Update Location for GPRS messages.

For the FUNCTIONAL_SS_CONTEXT and NETWORK_UNSTRUCTURED_SS_CONTEXT, the ngHLR's process is not changed by this feature, it just continues to use the Map Open Destination reference to extract the IMSI or MSISDN and then use the proper associated HLR Number.

Behavior of ngHLR

The ngHLR finds the correct HLR Number to return in the SCCP's Calling Address of the MAP response, based on the following factors:

1. Activation of the Enhanced Control Of SCCP Routing feature.
2. The format, the translation type or the numbering plan and nature of address of the SCCP's Called Address of the MAP request.
3. The detection of a number portability prefix in the SCCP's Called Address of the MAP request.
4. Match of the SCCP's Called Address found with a subscriber profile's data:
    a. Best match found of the MSISDN received in the database's MsIsdnlmsiProfileAssociation table. The IMSI associated to the MSIDN received is the one used to find the correct HLR Number.

b. Best match found of the received or extracted IMSI with an IMSI range in the IntraPlmnImsiRange table. The HLR Number associated to the IMSI range with the best match found is the one returned in the MAP response.

5. Match of the SCCP's Called Address of the MAP request not found with a subscriber profile's data:

   a. Exact match found of the SCCP's Called Address of the MAP request with a HLR Number in the HlrNumberConfig table in the database.
   b. First match found of the CC/NDC in the HlrNumberConfig table in the database.

Depending on these factors, the ngHLR will return one of the following as the SCCP's Calling Address in the MAP response:

- The HLR Number associated to the IntraPlmnImsiRange table's IMSI range, that best matches the received or extracted IMSI.
- The first HLR Number in the HlrNumberConfig table that matches the received CC-NDC.
- The default HLR Number from the HlrNumberConfig table. The default HLR Number is the one with the smallest ID.
- The exact same number received as the SCCP's Called Address of the MAP request.

What follows is a more detailed description of the ngHLR's behavior depending on the activation of the Enhanced Control Of SCCP Routing feature:

When the Enhanced Control of SCCP Routing feature is deactivated

If, upon receiving a MAP message, the ngHLR verifies that the feature is deactivated then two scenarios can occur:

- If the feature is deactivated and the Calling SSN does not correspond to a VLR or SGSN, then the SCCP's Calling Address of the response will be the SCCP's Called Address of the Request.
- If the feature is deactivated and the Calling SSN corresponds to the VLR or SGSN, the ngHLR performs the following verifications depending on the MAP request's Called party address's Numbering Plan:
- In the case where the Numbering plan is E.212, the ngHLR verifies if the IMSI has a best match in the IntraPlmnImsiRange[] table:
  - If a best match is not found, then the SCCP's Calling Address of the response will be the SCCP's Called Address of the Request.
  - If a best match is found, then the ngHLR returns, in the SCCP's Calling Address of the response, the HlrNumberConfig value associated to the IntraPlmnImsiRange[] table's best matched IMSI range value.
- In the case where the Numbering Plan is E.214 or E.164, the ngHLR verifies if the SCCP's Called Address of the MAP request digits have an exact match with one of the HLR Number values configured in the HlrNumberConfig[] table.
  - If there is an exact match, then the SCCP's Calling Address of the response will be the SCCP's Called Address of the Request.
  - If there is no exact match, then the ngHLR searches for the first match between the incoming message's CC/NDC and a HLR Number value configured in the HlrNumberConfig[] table.
    - If a match is found, then the SCCP's Calling Address of the response will be the HlrNumberConfig[]'s first HLR Number that matches the receiving CC/NDC.
    - If no match is found, then the SCCP's Calling Address of the response will be the SCCP's Called Address of the Request.

When the Enhanced Control of SCCP Routing feature is activated

- If the SCCP's Called Address MAP request's Global Title Indicator format is 2 (for ANSI systems), the ngHLR follows these steps:

1. If the Translation type is 10 or 14, then the ngHLR considers the MAP request Called party's Numbering Plan to be ISDN Telephony E.164. If the Translation type is 9, then the ngHLR considers the MAP request SCCP's Called party's Numbering Plan to be Land Mobile E.212.
2. If the incoming message SCCP's Called Party address is in Land Mobile E.212, then the ngHLR directly uses the received IMSI to select the proper IMSI range in the database's IntraPlmnImsiRange[] table. From the best matched IMSI range, the associated HLR Number is selected to use as the SCCP's Calling address of the response. In the case where no match is found between the received IMSI and the IMSI range entries in the IntraPlamnImsiRange[] table, the ngHLR returns the default HlrNumberConfig value* as the HLR Number in the SCCP's Calling Address MAP response.

   Note: *The default HlrNumberConfig value is the one with the smallest ID number.

3. If the incoming message SCCP's Called party address is in ISDN Telephony E.164, the system will look if this MSISDN matches any subscriber, by searching for an MSISDN match in the MsIsdnImsiProfileAssociation[] table. If a match is found, then the proper IMSI is extracted (the current active GSM IMSI if active, or the current active GPRS IMSI, or the Primary IMSI). From the best matched IMSI range found in the IntraPlmnImsiRange[] table, the associated HLR Number is selected to be used as the SCCP's Calling address of the response.

   Note: The system's provisioning validations ensure that each MSISDN be associated with an IMSI and that each provisioned IMSI matches an IMSI range with an HLR Number associated to it. Thus, once the system has found a match with one of its subscriber profiles (MSISDN present in database), it will always be able to find the IMSI, which will also always have an IMSI range with a HLR Number associated to it.

- If the MAP request's Global Title Indicator format is 4, (for ITU systems), then the ngHLR follows these steps:

  The system obtains the Numbering plan of the incoming SCCP called address.

  If the incoming message SCCP Called Party address's Numbering Plan is not ISDN Telephony E.164, then the ngHLR follows the same steps as the ones used when the feature is deactivated (except that ngHLR will not check if the message is from a VLR or SGSN).

  If the incoming SCCP called party address's Numbering Plan is ISDN Telephony E.164, then the ngHLR follows these steps:

  1. The ngHLR verifies if its Nature of Address (NOA) is International or not. In the case where the incoming Called Address's NOA is International.

     The ngHLR verifies if the following conditions are met:

     a. 1) the filteringCalling/PartyCheck and PrefixStrip attributes are activated (set to 1) in the EnhancedControlOfSccpRoutingConfig[] table

        2) the incoming message's called address begins with FilteringPrefix (prefix configured in the EnhancedControlOfSccpRoutingConfig[] table).

        In the case where the NOA is International and where these two conditions are met, the ngHLR removes the prefix by removing the first digits of the called party address as per the PrefixStripMsIsdnLength digits configured in the EnhancedControlOfSccpRoutingConfig[]

table. This allows the ngHLR to retrieve the MSISDN from a SCCP called party address that has a number portability prefix. In the case where the NOA is International, but the conditions 1 and/or 2 are not met, the ngHLR skips the removal of the prefix part.

b. The ngHLR then attempts to match the MSISDN with the MsIsdnImsiProfile Association[] table in order to find the associated IMSI.

c. The ngHLR uses the extracted IMSI (the current active GSM IMSI if active, or the current active GPRS IMSI, or the Primary IMSI) to find the best match with an IMSI range in the IntraPlmnImsiRange[] table.

If there is a match, then the HLR Number associated to the best matched IMSI Range is used as the SCCP's Calling address of the response.

In the case where the incoming SCCP's Called party address's NOA is not International or if there is no matching MSISDN in the MsIdnImsiProfileAssociation[] table:

2. The ngHLR verifies if the SCCP's Called Address of the MAP request digits have an exact match with one of the HLR Number values configured in the HlrNumberConfig[] table. In this case here are the possible scenarios:

- If there is an exact match, then the SCCP's Calling Address of the response will be the SCCP's Called Address of the Request.
- If there is no exact match, then the ngHLR searches for the first match between the incoming message's CC/NDC and a HLR Number value configured in the HlrNumberConfig[] table.
  - If a match is found, then the SCCP's Calling Address of the response will be the HlrNumberConfig[]'s first HLR Number that matches the receiving CC/NDC.
  - If no match is found, then the SCCP's Calling Address of the response will be the default HlrNumberConfig value* SCCP Called Address of the Request.

    Note: *The default HlrNumberConfig value is the one with the smallest ID number.

- If the MAP request's SCCP Global Title Indicator format is not 2 or 4, then the ngHLR follows the same steps as the ones for when the feature is deactivated (Except that the ngHLR does not check if the message is from a VLR or SGSN.)

This figure shows a graphic of the way the SCCP routing is controlled.

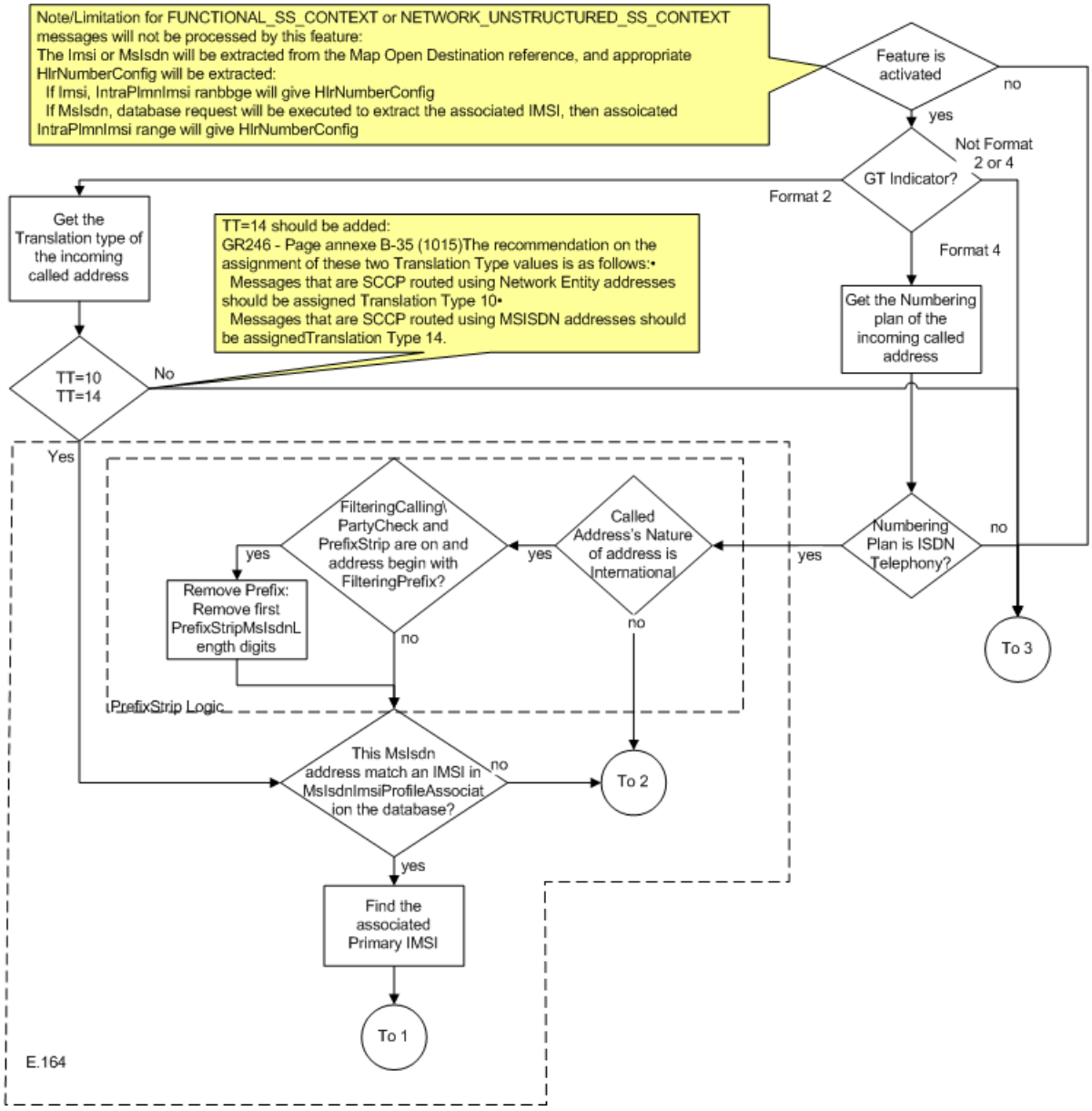
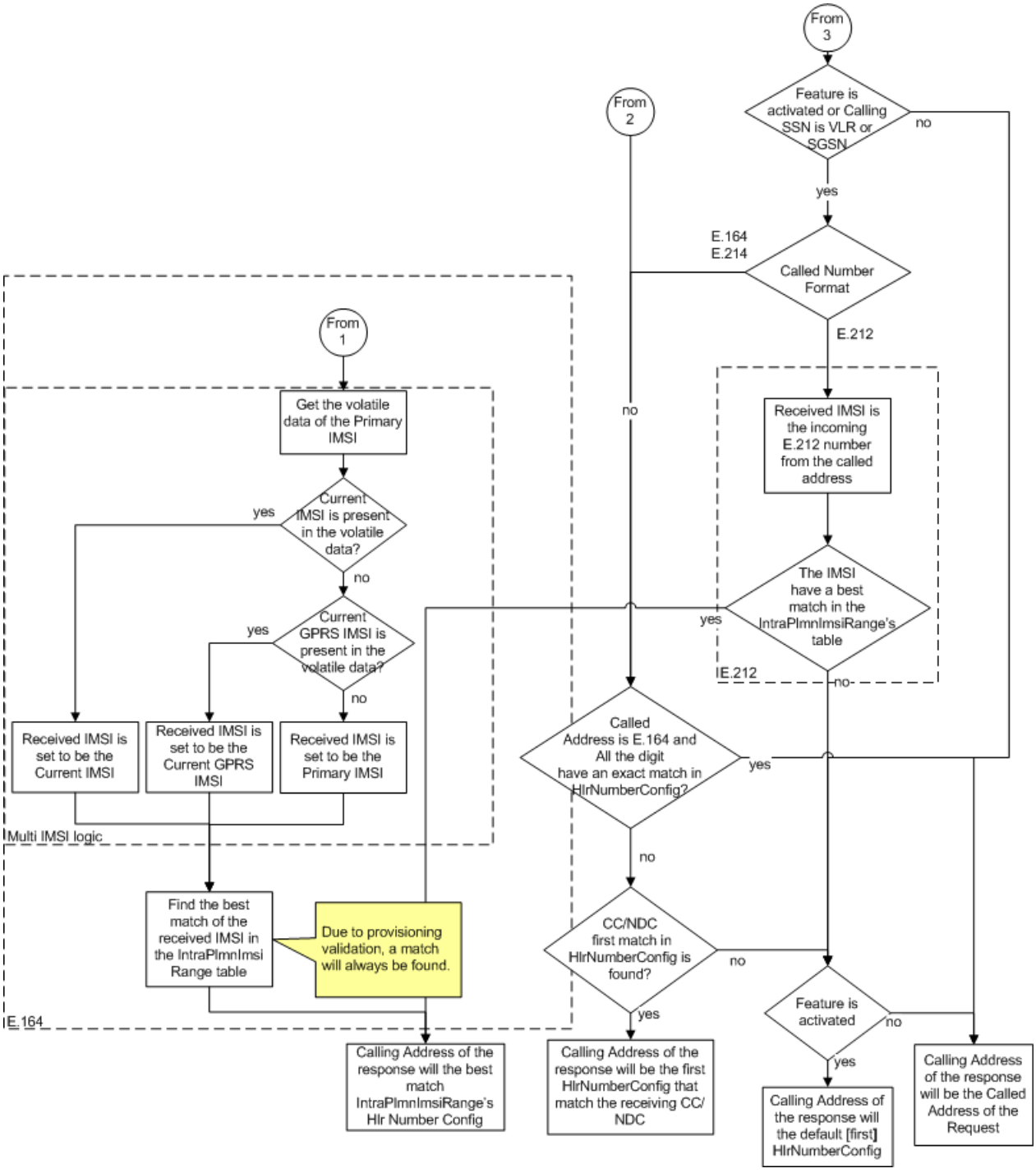


Figure 30: SCCP Routing for ITU and ANSI Calls



SCCP routing controls provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 22: Provisioning Information - SCCP Routing Controls

Affected Components	Description	Reference
Provisioning Interfaces	CLI, WebCI, XML interfaces: XML	
Tables[]/ attributes	• To enable/disable the support of the SCCP routing feature provision the ActivateFeature() or DeactivateFeature() operations in the HlrConfig[] table.	*SDM System Configuration Reference Manual:* • *HLR Operations* *SDM System Configuration User Guide:* • *Viewing the activation status of HLR features and activating/deactivating them individually*
	• To to show the activation status of the SCCP Routing feature the EnhanceControlOfSccpRouting and UpdateOfSccpCgAddrOnlyForUL parameters need to be activated in the HlrConfig[] **Note:** This script should be disabled to have the EnhanceControlOfSccpRouting feature to work properly.	*SDM System Configuration User Guide:* • *Provisioning/Modifying the Enhanced Control Of SCCP Routing Configuration*
	• To define SCCP Routing feature provision the EnhancedControlOfSccpRoutingConfig[] (for example, FilteringCallingPartyCheck, FilteringPrefix, PrefixStrip, PrefixStripMsIsdnLength. **Note:** the filtering prefix logic is only applicable for the ITU system because the ANSI system will not accept it.	*SDM System Configuration User Guide:* • *Provisioning/Modifying the Enhanced Control Of SCCP Routing Configuration*
Alarms	None	*Alarm Dictionary*
Error Messages	None	*SDM Monitoring, Maintaining, Troubleshooting Reference Manual*
Counters	None	*SDM Monitoring, Maintaining,*

Affected Components	Description	Reference
		Troubleshooting Reference Manual
Procedures	Provisioning the SCCP Routing Controls • *Provisioning/Modifying the Enhanced Control Of SCCP Routing Configuration*	• *SDM System Configuration User Guide:* • *Provisioning/Modifying the Enhanced Control Of SCCP Routing Configuration*

Entity to hold generic values

The SubscriptionGenericData[ ] entity has been implemented to give to the Network Operator the possibility to provision extra data for a subscriber (SubscriptionID). This entity contains two attributes: GenericName and GenericValue. GenericName is a mandatory attribute and can take any name up to 32 bytes. GenericValue can take any value up to 1024 bytes. The entity is associated with a SubscriptionID and can be provisioned via the CLI or using XML scripts (via CFL, SOAP/XML).

Refer to the "Subscription Generic Data" section of the *SDM Subscriber Provisioning - Reference Manual* for more details on the SubscriptionGenericData[ ] entity.

HLR overload control

The following types of overload control have been implemented in the Tekelec ngHLR:

- Dialog
- CPU

The Dialog Overload consists of monitoring the amount of open transactions in the Hlr process. If the amount of dialog exceeds the configured threshold (currently set to 1500), the "`OverloadControlDlg`" alarm (ID:`9039`) is generated and the system becomes in overload mode.

The CPU Overload consists of monitoring the CPU usage of the Hlr process. If the CPU exceeds the configured threshold (currently set to 240%), the "`OverloadControlCpu`" alarm (ID: `9038`) is generated and the system becomes in overload mode.

When the system is in overload mode, any request to open a new dialog is rejected by the system ("`MAP REFUSE`" with no reason is sent to the originator).

As soon as the system is back below the overload threshold, the overload condition is reset, and the system goes back to a full operational state.

Note: The alarm is cleared a minute following the reset of the overload state.

If the system is continuously in and out of an overload mode, the Tekelec ngHLR computes the amount of seconds the service is in overload, and if this period of time exceeds the threshold of 30 seconds (over a 60 second period), then the "`OverloadControlUOS`" alarm (ID:`9040`) is generated and the

TCAP layer is disabled for a short amount of time, during which all the incoming messages are rejected by the SCCP with the "`SubSystem Prohibited`" reason.

The Tekelec ngHLR monitors the dialog and CPU and when they are both underneath a pre-defined threshold, the " `OverloadControlUOS`" alarm is cleared and the TCAP layer is restarted:

- When the CPU goes back down lower than the CPU threshold.
- When the amount of dialog is less than the Dialog Threshold. This Dialog Threshold has been implemented to monitor the dialog and trigger when this overload mode can be reset.

For further details on these alarms, refer to the *SDM Alarm Dictionary*.

SIP-based SimRing

This feature allows the Network Operator to configure subscriptions as such that upon the reception of a voice call for a subscription's "Main" MSISDN, up to 10 devices (GSM based, PSTN based, SIP based, etc.) could ring simultaneously. The first destination to be answered is connected and the other ones are dropped.

For example, the figure shows that

- Incoming SMS to “Main” is directed to the primary user only.
- Incoming voice calls to “Main” cause all phones to ring.
- Optional - each phone can be reached on a direct number (no simring).
- Outgoing calls/SMS can have Main or specific number (configured in profile).
- Each user has a separate service profile (i.e., forwarding, barring, roaming, etc).
- One subscription is defined with the “Main” MSISDN and with as many Simring numbers as desired (currently limited to 10).

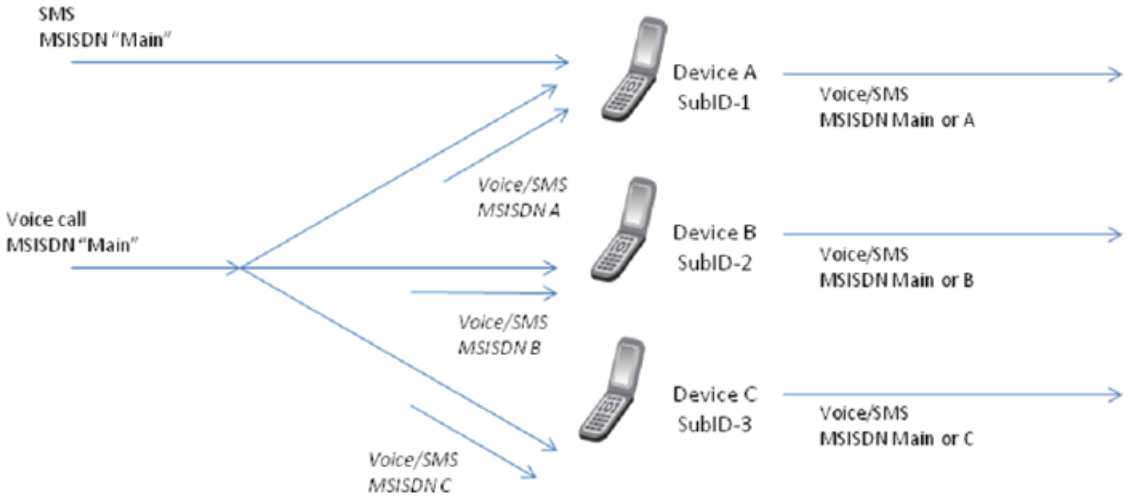


Figure 31: SIP-based SimRing

Since the SRI response can only send one number, the Tekelec ngHLR uses the SIP application properties to ultimately be able to fork the call to multiple devices. More precisely, the Tekelec ngHLR behaves as follows:

- Upon receiving an SRI message for a voice call with the “Main” MSISDN, the Tekelec ngHLR skips the normal SRI procedure and performs right away a search of the VoIP DN provisioned as the

Directory Number in the AddressOfRecord list for the “Main” MSISDNs subscription (SubscriptionID). The Directory Number found will be returned as the „VoIP DN in the SRI-ack. This allows to transfer the request to the SIP Domain.

The „ForceToSip flag has been implemented in the MSISDN entity in order to allow the Network Operator to activate (ForceToSip=1) this behavior for a subscribers MSISDN. A MSISDN with the flag „ForceToSip set to „1 is said to be the “Main” MSISDN.

- An Invite message with the subscribers VoIP DN is then sent to the SIP Proxy, which can fork the call based on a 300 response from the Tekelec ngHLR's SIP application (SIP Redirection Override functionality) and then redirect each forked leg based on 302 responses. By initiating dialogue with the Tekelec ngHLR based on a SIP Invite (VoIP DN), the SIP Proxy can ultimately retrieve all the MSRNs based on 302 responses and then fork the call to all the required devices simultaneously, as per configured in the Tekelec ngHLR.

Note: The SimRing solution applies to voice calls only, even if an SMS is sent out for the “Main” MSISDN, it will not SimRing and will only be received by the device with the “Main” MSISDN. SMS can only be delivered to a single user.

In order to achieve this, the Network Operator must primarily define different subscriptions for each SimRing device. One of those subscriptions must be provisioned with a “Main” MSISDN and all the other SimRing numbers to be reached must be defined as AORs in the subscriptions SipRedirectionOverride entity. All the other subscriptions must each be provisioned with one of the SimRing numbers as an AOR in the AddressOfRecord entity.

More precisely, the Network Operator must configure the system as follows:

1. One “Main” MSISDN must be defined, by setting the subscriptions desired MSISDN to „ForceToSip=1 in the MSISDN entity.
2. Under the same subscription as the “Main” MSISDNs, the following must be configured:
   a. The „Reachable flag in the MsisdnImsiProfileAssociation entity must be set to „1 (true) for the “Main” MSISDN.
   b. The „Published flag in the MSISDN entity must be set to „1 (true) for the “Main” MSISDN (if not, the call fails and there is no SimRing).
   c. At least one AOR must be provisioned with a Directory Number in the AddressOfRecord entity. Make sure to provision the AOR with DN as follows:
      a. The „user field of the AOR must be exactly as the „Directory Number field.
      b. The „scheme and domain (identified by the AorDomainId) must be the same as the ones used by the networks SIP Proxy.

      If multiple AORs are provisioned with Directory Numbers, the Tekelec ngHLR uses the first Directory Number found in the AddressOfRecords table to return as the VoIP DN. If no AOR is found for the “Main” MSISDN, the call fails with „Absent Subscriber error. It is highly recommended that only one AOR be provisioned with a Directory Number.
   d. The SIP Redirection Override functionality must be enabled for the AOR corresponding to the “Main” MSISDN (AOR provisioned with a DN equal to the VoIP DN).
   e. The canonical URI of each SimRing number (each device that must be reached simultaneously) must be defined in the SipRedirectionOverride entity for the AOR provisioned with a Directory Number equal to the VoIP DN (for the “Main” MSISDN). Moreover, each SimRing group must be provisioned with the same q-value. The value „1 is recommended for highest priority and therefore immediate SimRing.

Note: Take note that if you wish to have the "Main" MSISDN ring simultaneously with the others, you must also provision a canonical URI for that SimRing number in the SipRedirectionOverride entity. All the canonical URIs provisioned in the SipRedirectionOverride entity for the "Main" MSISDN will be sent to the SIP Proxy by the Tekelec ngHLR in a 300 response.

3. Each canonical URI defined in the SipRedirectionOverride entity of the "Main" MSISDNs AOR (AOR with Directory Number=VoIP DN), must be defined exactly the same in the AddressOfRecord entity of different subscriptions except that the redirection override functionality shall be disabled. This means that the AddressOfRecords:
   a. *User*, *Scheme*, and *Domain* fields must match the canonical URI defined in the "Main" MSISDNs SIP Redirection Override entity.
4. It is important that each AOR belongs to a separate subscription (SubscriptionID), so that each device has different service settings and roaming entitlements.
5. A minimal service profile (SIM/IMSI/MSISDN/HLR Service Profile) is needed for each subscription (SubscriptionID) in order to be able to redirect the call to SIP and to respond to SIP Invite messages.

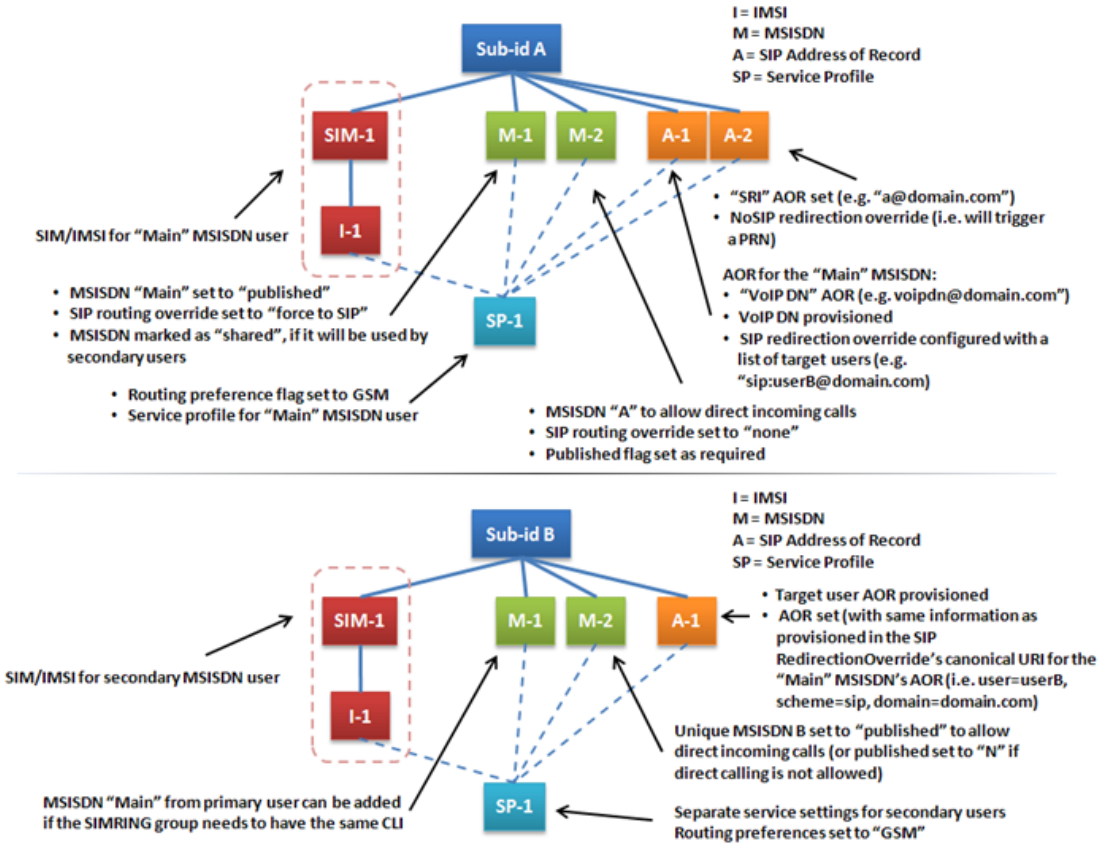


Figure 32: SimRing configuration

The SimRing solution can be used on its own, but also in variant contexts, such as the following:

- The „Shared MSISDN feature can be used within the SimRing solution if you wish for the CLI to be the same for each device within a SimRing group (group of devices that will be reached simultaneously for a voice call to the “Main” MSISDN). For example, in the case where you wish for the CLI to be the same as the “Main” MSISDN for a SimRing group, you must make sure you set the “Main” MSISDNs „Shared flag to „1 (true) and then make sure you define the same MSISDN as the “Main” one in each of the SimRings devices subscription profile.
- The sequence in which the devices are reached can be set by the Network Operator. Within the SimRing solution, this means that the Network Operator can set different devices to SimRing at different times when receiving a voice call for a “Main” MSISDN. For example, upon reception of a voice call for a “Main” MSISDN, two devices might be reached simultaneously in a first time and then if none of them have connected, a second group of devices could be reached simultaneously or the voicemail could be reached. To be able to achieve this, a q-value has been added to the SIP Redirection Override, which gives a priority order in which the devices must be reached (simultaneous or sequential ringing). The Network Operator can set the SipRedirectionOverride entitys „Qvalue parameter to any value between „0 and „1 („1 being the highest priority). Just keep in mind that the value of the q-value must be the same for each SimRing group.

In summary, the q-value allows to configure different SimRing groups (devices reached simultaneously as per the SimRing solution) for one “Main” MSISDN by setting the q-value to a different value for the two groups.

For more details on how to provision subscriptions with a service profile, the MSISDN entity, the AORs and the SIP Redirection Override, refer to the *SDM Monitoring, Maintaining, and Troubleshooting – User Guide*. For details on the „ForceToSip flag and on the „Qvalue , refer to the *MSISDN* section and the *SipRedirectionOverride* entity respectively in the *SDM Subscriber Provisioning – Reference Manual*.

Support profile with no MSISDN

The implementation of the 'Support profile with no MSISDN' feature allows the Network Operator to provision a Subscription without any MSISDN. This allows the Network Operator to create a profile for a subscriber that will only be used for IMSI based messages.

To allow this, a Subscription has been implemented with the following characteristics:

- SubscriptionID: NOMSISDN
- No profile
- No SIM
- No IMSI-MSISDN associations
- One single MSISDN set to the '0' value and with the 'Shared' flag set to '1' and the 'Published' flag set to '0' (not published).

This Subscription is part of the default values of the system, which means that it is always provisioned on the system.

Since the 'Shared' flag of the 'NOMSISDN' Subscription is set to '1', this special MSISDN (MSISDN=0) can be shared, which means it can be used by any other Subscription.

This allows the Network Operator to provision Subscriptions with only the SIM(s) and the service profile, but with no MSISDN and by associating its IMSI(s) with the special MSISDN (MSISDN=0) and setting the 'Displayed' flag to '1'. Associating an IMSI with the special MSISDN ('0') acts as if the corresponding IMSI has no MSISDN associated to it. This means that all IMSI based messages (e.g. UL, RegSS, etc) are processed as normally, but the subscriber cannot receive MSISDN based messages (e.g. SRI, SRI-SM, etc). In the case where the displayed MSISDN of the IMSI is '0', if an update location

or update location GPRS is received, the ngHLR sends an ISD message to the VLR or SGSN with the contents of the subscriber profile, but without the MSISDN parameter.

GSM/IMS Router

The Tekelec ngHLR can be configured as a GSM or IMS router using redirect or relay routing functionalities for the following messages:

- SRI MT-SMS
- SRI
- SRI-LCS
- ATI

The table indicates the routing type supported per message:

Message	Type of routing supported
SRI	Redirect/Relay
SRI-LCS	Redirect/Relay
SRI MT-SMS	Redirect/Relay
ATI	Relay

When one or more of the routing functionalities are activated (SriRouting, SmsRelay, or SmsRouting), the Tekelec ngHLR routes one of the supported messages to either the GSM or IMS networks depending on whether the mobile subscriber is SIP-, TAS-, or HLR-registered.

The messages can be routed to one of the following nodes:

- Destination Router (in the GSM network)
- External HLR (in the GSM network)
- External TAS (in the IMS network)

The Tekelec ngHLR processes the MAP request received for a subscriber per the Routing Controls configuration (Routing Exceptions, Destination Router, SIP TAS Gt) and per the Routing Template (routing type, routing trigger, default action) assigned to it. The Routing Template ultimately defines the routing type, the data the Tekelec ngHLR must include in the outgoing MAP message and the external node to which the message will be routed.

The Tekelec ngHLR relays the received MAP messages by simply transmitting them as follows:

- To a configured Destination Router or TAS: By changing the CdPA (Called Party) and Tt (Translation Type) to a configurable value. This process will be called Relay to Destination Router (also known as: Relay to Gt).
- To an external HLR: By keeping the same CdPA and changing the Tt to a configurable value. This process will be called the Default Relay with CdPA.

The Tekelec ngHLR redirects the received MAP messages by sending back a MAP Ack message including the following:

- For SRI MT-SMS/SRI-LCS/ATI: the IMSI and the Network Node Number (Gt of the Destination Router, as configured in the DestinationRouter or SipTasGt table.
- For SRI: the IMSI and MSRN (Redirect Prefix + MSISDN).

The Gt, Tt, Override Tt, and Prefix are all configurable in the Tekelec ngHLR's DestinationRouter table or in the SipTasGt table. The Tekelec ngHLR will retrieve these configured values from:

- The DestinationRouter table, if the subscriber has a Routing Template associated to it and is not TAS registered.
- The SipTasGt table. If the subscriber is TAS registered, the Tekelec ngHLR will use the data provisioned in the SipTasGt table for the TasId of the subscriber (TasId other than 0) as defined in the Registration Bindings. If the subscriber has no routing template associated to it and is not TAS registered, the Tekelec ngHLR will use the data provisioned in the SipTasGt table for the TasId=0 (entry in the SipTasGt table for subscribers that are not TAS registered).

Overall, upon receiving a MAP SRI MT-SMS, SRI, SRI-LCS or ATI message, the Tekelec ngHLR looks up in the database the activation status of the routing functionalities, the MSISDN received in the message, the routing template associated to it, the subscriber profile and the HLR volatile data (HLR registered) or SIP registration bindings (SIP registered (TasId=0) or TAS registered (TasId is not 0)). Based on this information, it will know where the subscriber is currently registered and be able to decide how to route the message (relay or redirect) and what information to include in the message (i.e Gt, Tt, NNN, MSRN).

Note: If the value of the Override Tt in the SipTasGt or DestinationRouter table is set to 0, the Tt value is not changed. If it is set to 1, the Tekelec ngHLR changes the received Tt with the Tt configured in one of these tables.

Finally, for this solution to be successful, the Tekelec STP must be used in conjunction with the Tekelec ngHLR. The Tekelec STP G-Flex database will ensure that the MAP messages are routed properly to the Tekelec ngHLR or to the correct external HLR/TAS/Destination Router. For more details on the Tekelec STP, contact the Tekelec *Customer Care Center*.

IMS Router Overview

This functionality allows mobile terminated calls from the cellular domain to be routed to a Telephony Application Server (TAS) when a subscriber is registered in the SIP/IMS domain.

Description

With the implementation of this functionality, the SIP Registrar can support registrations from a 3rd party, more specifically, it allows the SIP Registrar to receive SIP REGISTER messages from a TAS node. Upon registration, the system generates a SIP Registration Binding with the ID of the TAS (TasId) the SIP REGISTER message comes from.

The following items must be configured for the SDM system to perform all the functions associated with the IMS Router functionality:

- The SIP Server and HLR Server must both be configured and capable of actively running traffic.
- The SIP RegistrarConfig entity. For optimum performance, contact the Tekelec *Customer Care Center*.

SIP Server Functionality

The SIP Server functionality that supports the IMS Router implements the following capabilities:

- Support registrations from a 3rd party, more specifically, it allows the SIP Registrar to receive SIP REGISTER messages from a TAS node.
- Create SIP Registration Bindings for 3rd party registrations with a TasId.

This SIP functionality is available by default when the SIP Registrar server is activated. The functionality is invoked automatically when a 3rd party registration is detected at runtime.

Note that this functionality introduces limited support for 3rd party registrations when:

1. The "to" and the "from" headers are different. The following logic is applied:
   a. The FROM URI user part is NOT mandatory. If a user part is received, it is ignored.
   b. The 3rd party REGISTER is NOT rejected if the host part of the "from" header (i.e., TAS FQDN) is provisioned in the SipTasGt entity.
   c. If the 3rd party IMS REGISTER is detected but the TAS FQDN is not configured, the SIP REGISTER request is rejected with a 404 error message.
2. The "to" and the "from" headers are equal. Normal SIP Registration processing applies (SIP Registration process without the 'SRI Router' functionality).

A user can have a single 3rd party registration binding (i.e., a maximum of one registration with a non-zero TasId). If a re-registration for a user occurs from a different TAS (i.e., a different "from" header), the Registration Binding is overwritten since it is from the same user (i.e., the same "to" header). A RegistrationBinding is deleted when a DE-REGISTER is received or when the RegistrationBinding cleanup is activated and the RegistrationBinding is expired (see *Registration Binding Cleanup* for more details).

The REGISTER/DE-REGISTER call flow is depicted in *Figure 33: Register/De-Register Call Flow in the IMS Domain for 3rd Party Registration from TAS Node*.

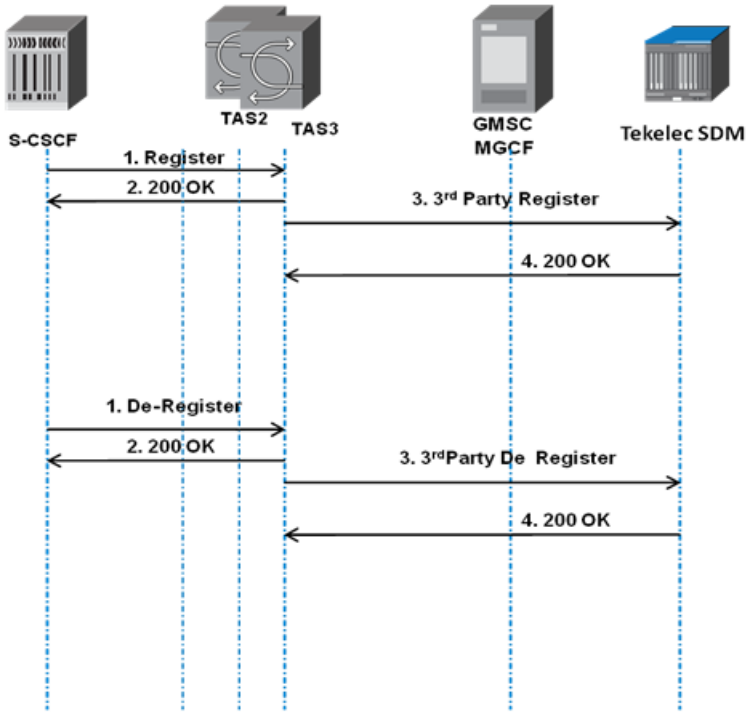


Figure 33: Register/De-Register Call Flow in the IMS Domain for 3rd Party Registration from TAS Node

HLR Server Functionality

The HLR Server functionality that support the IMS Router mainly consists of an addition to the MAP SRI, SRI-LCS, ATI and MT-SMS processes mechanism to relay the MAP messages based on the TAS ID (TasId) of the 3rd party SIP registration bindings. To determine whether a subscriber is TAS registered

or not, the Tekelec ngHLR looks up the TAS ID in the subscriber's SIP registration bindings. If the TAS ID is 0 (TasId=0), the subscriber is not considered to be TAS registered. If the TAS ID is not 0 (TasId≠0), the subscriber is considered to be TAS registered.

The Registration Binding cleanup (expiration) affects the HLR Server's database request to find the TasId. If the RegistrarConfig entity's 'IsExpiryTimestampSet' attribute is set to '1' (Registration Binding cleanup enabled), the HLR Server tries to find the TasId in SIP registration bindings, but only if the 'RegistrationExpiryTime' is greater than the current time. If the 'IsExpiryTimestampSet' flag is set to '0' (Registration Binding cleanup disabled), the HLR Server does not verify the 'RegistrationExpiryTime'.

Registration Binding Cleanup

The Registration Binding cleanup mechanism deletes expired registration bindings and ultimately increases the performance of the system. By configuring the RegistrarConfig entity, the Network Operator has full control of the activation of this mechanism, its execution time, and of the enabled/disabled status of the expiry timestamp of the registration bindings.

GSM/IMS Router Provisioning

Provisioning

The SDM provisioning interfaces allow the Network Operator to:

- Activate/deactivate one or several of the routing functions (SRI Routing, SMS Relay, SMS Routing)
- Define a list of Destination Router addresses (used if mobile device is HLR or SIP registered) and/or a list of SIP TAS Gt (used if mobile device is TAS registered).
- Define various Routing Templates, which specify how the Tekelec ngHLR will process the MAP messages:
  - Define Routing Type (Relay or Redirect)
  - Define Routing Trigger
  - Define Default Action
  - Associate one of the Destination Router addresses
- Define a list of Originator SMS-GMSC as exceptions and from which no MAP SRI-for-SM shall ever be routed.
- Associate a Routing Template to MSISDNs to control the MAP Routing process on a per-subscriber basis. HLR subscriber profiles can also be provisioned with a Routing Template, but the latter is only used for MT-SMS Routing.
- Define an IMSI for each of a subscriber's MSISDNs in the IMSIForRedirectRouting table. This step is very important in the cases where the Tekelec ngHLR doesn't know the IMSI of the subscriber. This can occur in the following cases:
  - there is no full subscriber profile provisioned in the Tekelec ngHLR for the subscriber (e.g., only MSISDNs)
  - the subscriber is not registered.

  In order to return the mandatory IMSI parameter in the MAP SRI MT-SMS Ack message, the Tekelec ngHLR first reads the IMSI provisioned in the IMSIForRedirectRouting table and if no IMSI is provisioned, it returns the default IMSI configured in the DestinationRouter or SipTasGt table. This behavior ensures that the MAP Forward SM contains the necessary information to correctly identify the subscriber.

Feature Activation

The GSM/IMS routing functions can be activated at a high level for the entire Tekelec ngHLR. They can also be activated on a per subscriber basis by assigning or not assigning a Routing Template to MSISDNs (and/or to a HlrServiceProfile for the MT-SMS Routing functionality).

By default, the GSM/IMS Routing functions are unavailable and the Tekelec ngHLR follows the standard MAP message processing. Contact the Tekelec *Customer Care Center* to make the GSM/IMS Routing functionalities available to the Network Operator for dynamic activation or deactivation.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 23: Provisioning Information - Routing Functionalities

Affected Components	Description	Reference
Provisioning Interfaces	CLI, XML, XML-SOAP, WebCI	

Main Tables[]/ attributes	• To activate/deactivate routing functionalities, the following attributes must be set in the HlrConfig[] table:
	  • `SmsRouting` - for MT-SMS Redirect functionality
	  • `SmsRelay` - for MT-SMS Relay functionality
	  • `SriRouting` - for SRI/SRI-LCS/ATI functionalities
		SDM System Configuration Reference Manual:
		• *HLR Configuration*

	• To define a list of Destination Router addresses and related data (i.e., Gt, Tt, Prefix, Override Tt):
	  • `DestinationRouter[]`
	• To define exception addresses (only applies for MT-SMS messages):
	  • `RoutingExceptions[]`
	• To define Routing Templates (Routing ID, trigger, type, default action, destination router, routing exceptions):
	  • `RoutingTemplate[]`
	• To define a subscriber IMSI (only applies for MT-SMS messages):
	  • `IMSIForRedirectRouting[]`
	`
		SDM System Configuration Reference Manual:
		• *Routing Controls*

Affected Components	Description	Reference
	• To define a list of TAS Gt addresses and related data (e.g., Gt, Tt, Prefix, TasId, Tas FQDN,OverrideTt): • `SipTasGt[]` • To define SIP domains *Request-URI domain* and *TO URI domain* before the HLR service is started: • `Domain[]`	*SDM System Configuration Reference Manual:* • *SIP Server Configuration*
	• To support 3rd-party registrations and increase system performance by controlling the registration bindings (e.g., delete expired ones, set a maximum number of contacts): • `RegistrarConfig[]` • MaxContactsPerAor - maximum contacts in RegistrationBinding for same user • MinRegistrationDuration - minimum expiration duration • MaxRegClients - maximum number of simultaneous Register messages handled • IsExpiryTimestampSet - enable/disable Expiry Timestamp • IsRegistrationCleanupEnable - dynamically enable/disable Registration Binding cleanup mechanism • RegistrationBindingCleanupTime • To view 3rd-party registrations from TAS nodes: • `RegistrationBinding[]` • `TasId`	*SDM System Configuration Reference Manual:* • *SIP Registrar Configuration*
	• To associate routing template(s) to a subscriber's MSISDN(s), the following attribute(s) must be provisioned in the MSISDN[] entity: • SmsTemplateId And/Or • SriTemplateId	*SDM Subscriber Provisioning Reference Manual:* • *Home location Register (HLR), MSISDN Provisioning*

Affected Components	Description	Reference
Alarms	**SRI:** • 9143-SriRoutingActivated • 9144-SriRoutingDeactivated	*Alarm Dictionary*
Error Messages	None	---
Counters	**SMS:** • 12239-SmsReceived • 12240-SmsRegistered • 12241-SmsNotRegistered • 12242-SmsNotFound **SRI:** • 10010 RegisterImsrTasNotFound • 12203-SriRoutingSriReceived • 12204-SriRoutingSriRegistered • 12206-SriRoutingSriNotRegistered • 12207-SriRoutingSriNotFound • 12205-SriRoutingNonSri • 12237-SriRoutingSriRelayed • 12238-SriRoutingSriRedirected **SRI LCS:** • 12222-SriLcsMsisdnInd • 12223-SriLcsImsiInd • 12224-SriLcsRsp • 12225-SriLcsNeg • 12226-SriRoutingSriLcsReceived • 12227-SriRoutingSriLcsRelayed • 12228-SriRoutingSriLcsRedirected • 12229-SriRoutingSriLcsRegistered • 12230-SriRoutingSriLcsNotRegistered • 12231-SriRoutingSriLcsNotFound **ATI:** • 12232-SriRoutingAtiReceived • 12233-SriRoutingAtiRelayed • 12234-SriRoutingAtiRegistered • 12235-SriRoutingAtiNotRegistered • 12236-SriRoutingAtiNotFound	*Performance Measurements*

Affected Components	Description	Reference
Procedures	• *Activating/deactivating HLR features or functionalities* • *Provisioning Routing Controls for GSM/IMS Router capabilities* • *Viewing and editing SIP TAS configuration for 3rd party registration*	*SDM System Configuration User Guide*
	• Provisioning MSISDNs: *Viewing/Editing SIM Cards, MSISDNs, IMSIs and HLR Subscriber Profiles* • Provisioning HLR Service Profile: *Viewing/Editing a HLR Service Profile* • Provisioning SIP subscriber profile: *Viewing/Editing SIP Subscriber Profiles (Address Of Records)*	*SDM Monitoring, Maintaining, Troubleshooting User Guide*

	• *Examples of XML Templates for Subscriber Provisioning*
	  • *HLR subscriber profile provisioning template*
	  • *SIP subscriber profile provisioning*
		SDM Subscriber Provisioning User Guide

Routing Process

Based on various factors, the Tekelec ngHLR may treat the MAP message by using the corresponding standard process or Routing Template process. This section describes the logic used by the Tekelec ngHLR to determine which process it follows to proceed with the MAP message.

Upon receiving one of the MAP messages supported for routing (SRI/SRI-LCS/ATI/MT-SMS), the Tekelec ngHLR :

- Verifies that the MNP functionality is not activated and that the subscriber is not ported out. If otherwise, the Tekelec ngHLR proceeds this message with the MNP process.
- Verifies that the SSR functionality is not activated. If otherwise, the Tekelec ngHLR proceeds this message with the SSR process.
- Verifies the activation state of the SriRouting and SmsRouting functionalities. If these functionalities are deactivated, the Tekelec ngHLR proceeds with the standard MAP process.
- Looks up in its database the MSISDN received in the MAP message. If the MSISDN is not found in the database, the Tekelec ngHLR defines the MSISDN as unknown. At this point, the Tekelec ngHLR performs the following:
  - Responds to a MT-SMS message with the "MAP Unknown Subscriber" message.
  - If the MAP message received is SRI/SRI-LCS/ATI, the Tekelec ngHLR verifies whether the SriRouting activation state is set to 'Template Only' or not. If the state is set to 'Template Only', the Tekelec ngHLR proceeds with the standard processing and replies with a "MAP Unknown Subscriber" message. If the state is not set to 'Template Only' (either set to Relay or Redirect), the Tekelec ngHLR performs a default Relay to the appropriate external HLR.

    Note: If the SRI-LCS message received does not include the MSISDN, but instead the IMSI, the Tekelec ngHLR considers the MSISDN as unknown and proceeds with the verification of the SriRouting activation state (as described earlier).

- When the MSISDN is found in the database, the Tekelec ngHLR verifies the provisioned setting of the SmsTemplateId or SriTemplateId in the MSISDN table or HlrServiceProfile:
  - SmsTemplateId:
    - The Tekelec ngHLR verifies the value of the SmsTemplateId in the MSISDN [] table first and if it is set to 'Not Defined' (0), it then verifies the value of the SmsTemplateId in the HLR Service Profile's SubscriberProvisioning[] table. The Tekelec ngHLR considers that the subscriber is not associated to any routing template if the SmsTemplateId is set to 'NotDefined' (0) in both of these tables. In this case, the Tekelec ngHLR continues processing the message with the standard MT-SMS process.
    - The Tekelec ngHLR verifies the value of the SmsTemplateId in the MSISDN[] table first and if it is set to a supported value given for a provisioned Routing Template entry, the Tekelec ngHLR considers that a Routing Template is present for the subscriber. If it is set to 'Not Defined' (0) in the MSISDN[] table, it then verifies the SmsTemplateId value provisioned in the subscriber's HLR Service Profile's SubscriberProfile[] table. If it is set to a supported value that refers to a Routing Template entry in the RoutingTemplate[] table, the Tekelec ngHLR uses that value to make the association between a subscriber and a routing template. The Tekelec ngHLR then verifies if the subscriber profile is full. A full subscriber profile consists of at least an MSISDN, an IMSI and a SIM, as well as a SimImsiMap, an HlrServiceProfile and a MsisdnImsiProfileAssociation. For the MAP messages in the IMS network, this consists of an MSISDN only. If the subscriber profile is in fact full, it then continues processing the message with the MT-SMS Routing Template process. However, if the subscriber profile is not full, the Tekelec ngHLR verifies the activation state of the Sms Relay functionality:
      - If the Sms Relay functionality is activated, the Tekelec ngHLR continues processing the message with the MT-SMS Routing Template process, as per the routing template's settings (routing trigger, routing type, routing destination address, default action, etc.).
      - If the Sms Relay functionality is not activated, the Tekelec ngHLR continues processing the message with the standard MT-SMS process and returns a "MAP Unknown subscriber" error message.

    Note: The SmsTemplateId cannot be set to an empty (NULL) value.

  - SriTemplateId:
    - If the SriTemplateId is empty (Null), the Tekelec ngHLR verifies the activation state of the SriRouting functionality:
      - If the state is set to 'Template Only', the Tekelec ngHLR continues processing the message with the standard SRI/SRI-LCS/ATI process, as per the routing template settings (routing trigger, routing type, routing destination address, default action, etc.).
      - If the state is set to 'Redirect', the Tekelec ngHLR verifies if the subscriber is TAS registered. If the subscriber is TAS registered, the Tekelec ngHLR redirects the message to the appropriate TAS. If the subscriber is not TAS registered, the Tekelec ngHLR uses the default relay action and relays the message to the appropriate external HLR.
      - If the state is set to 'Relay', the Tekelec ngHLR verifies whether the subscriber is TAS registered. If the subscriber is TAS registered, the Tekelec ngHLR relays the message to the appropriate TAS. If the subscriber is not TAS registered, the Tekelec ngHLR uses the default relay action and relays the message to the appropriate external HLR.
    - If the SriTemplateId is set to a supported value given for a provisioned Routing Template entry, the Tekelec ngHLR continues processing the message with the SRI/SRI-LCS/ATI

Routing Template process per the routing template settings (routing trigger, routing type, routing destination address, default action, etc.).

When following the Routing Template processes, the Tekelec ngHLR bases itself on the settings configured for the subscriber's associated Routing Template.

Routing Template

The Routing Template provisions the following attributes:

- **Routing Type**

  The Tekelec ngHLR reroutes Map messages based on the configured routing type defined for each Routing Template:

  - Redirect
  - Relay

  Note: ATI messages cannot be redirected.

- **Routing Trigger**

  - *Never* - The Tekelec ngHLR never routes (relays/redirects) MAP messages to a configured Destination Router for the subscriber. The message follows the Tekelec ngHLR's default action configuration, which means that it is either processed locally with the Tekelec ngHLR's standard processing, or it is relayed with the CdPA to an external HLR.
  - *Always* - The Tekelec ngHLR always routes MAP messages to a configured Destination Router based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.
  - *When roaming out of HPLMN* - The Tekelec ngHLR routes MAP messages to a configured Destination Router if the subscriber is roaming out of the Home PLMN.
  - *When SIP registered* - The Tekelec ngHLR routes MAP messages to a configured Destination Router depending on the network in which the subscriber is currently registered in. It first checks if the subscriber is TAS registered, if not, it then checks if it is SIP registered and behaves as follows:

    - If the subscriber is TAS registered, the Tekelec ngHLR routes (relays/redirects) the message to an external TAS based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.
    - If the subscriber is not TAS registered but is SIP registered, the message is sent to a configured Destination Router based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.
    - If the subscriber is not SIP registered and not TAS registered, the message is routed to the Tekelec ngHLR's default action configuration. This means that it is either processed locally with the Tekelec ngHLR's standard processing, or it is relayed with the CdPA to an external HLR.

  - *When SIP registered or roaming out of HPLMN* - The Tekelec ngHLR checks the following:

    - TAS Registration

      - If the subscriber is TAS registered, the Tekelec ngHLR relays or redirects the message to the external TAS based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.

- If the subscriber is SIP registered and not TAS registered, the message is sent to a configured Destination Router based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.
- If the subscriber is not SIP registered and not TAS registered and is roaming out of the HPLMN, the message is sent to a configured Destination Router based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.

- Roaming out of HPLMN

  If the subscriber is not TAS registered and not SIP registered and is not roaming out of the HPLMN, the Tekelec ngHLR routes the message to the Tekelec ngHLR's default action configuration. This means that it is either processed locally with the Tekelec ngHLR's standard processing, or it is relayed with the CdPA to an external HLR.

- *When in the HPLMN* - The Tekelec ngHLR routes MAP messages to a configured Destination Router if the subscriber is registered within the HPLMN. The message is routed based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.
- *When SIP registered or in the HPLMN* - The Tekelec ngHLR checks the following:

  - TAS Registration

    - If the subscriber is TAS registered, the Tekelec ngHLR routes the message to the external TAS based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.
    - If the subscriber is SIP registered and not TAS registered, the message is sent to a configured Destination Router based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.

  - Roaming in the HPLMN

    - If the subscriber is not TAS registered and not SIP registered and not roaming in the HPLMN, the Tekelec ngHLR routes the message to the Tekelec ngHLR's default action configuration. This means that it is either processed locally with the Tekelec ngHLR's standard processing, or it is relayed with the CdPA to an external HLR.
    - If the subscriber is not TAS registered and not SIP registered and in the HPLMN, the message is sent to a configured Destination Router based on the Routing Template provisioned for the subscriber's MSISDN or subscriber profile.

- **Default Action**

  If a condition in the routing trigger is not met, the Tekelec ngHLR processes the message using the configured default action:

  - *Process locally* - the MAP message is processed using the Tekelec ngHLR's standard MAP processing.
  - *Relay with CdPA* - the MAP message is relayed to an external HLR using the same Gt (global title) but with a different Tt (translation type). The Tt used is as follows:

    - If the subscriber has a routing template provisioned in the Tekelec ngHLR, the Tt included in the message is the one provisioned in the Destination Router table.
    - If the subscriber does not have a routing template provisioned in the Tekelec ngHLR, the Tt included in the message is the one provisioned in the SipTasGt table for the TasId=0.

Note: When receiving a MAP message for a subscriber with no Routing Template provisioned (SmsTemplateId='Not Defined' (0) and/or SriTemplateId = '' (Null)), the Tekelec ngHLR follows the standard MAP processing to respond to the message.

Routing Conditions

The Tekelec ngHLR will successfully route the MAP messages if the following main conditions are met:

- The Tekelec ngHLR must be activated and configured with the HLR and SIP applications.
- MNP

  The MNP function must be deactivated and the subscriber must not be ported out. If activated the SDM handles the message as per the MNP process. The SDM will not route the MAP SRI-for-SM if the MNP is activated and the subscriber is ported out.

- SSR

  The SSR function must be deactivated. If activated then the SDM handles the message as per the SSR process. The SDM will not route the MAP SRI-for-SM if the SSR is activated.

- Activation of the Routing functionalities
  - The SRI Routing functionality must be activated (HlrConfig entity's SriRouting flag must be set to 1,2 or 3) in order to activate the Tekelec ngHLR's SRI/SRI-LCS/ATI routing capabilities.
  - Both the MT-SMS Redirect and Relay functionalities must be activated (HlrConfig entity's SmsRouting and SmsRelay flags must be set to 1) in order to activate the Tekelec ngHLR's MT-SMS routing capabilities. If the Routing function is deactivated then the SDM routes the MAP message to standard processing. If the Routing function is activated and the trigger of the template is not met, then, the message is processed locally and forwarded to the MSC/VLR, or it is relayed with CdPA to an external HLR.

- Routing Template

  A Routing Template must be associated with the MSISDN or with the HlrServiceProfile. If no routing template is present then the SDM routes the MAP SRI-for-SM message to standard processing. If there is no template defined for the subscriber, then, the message is processed locally and forwarded to the MSC/VLR, or it is relayed with CdPA to an external HLR.

- Subscriber Profile

  A full subscriber profile must be provisioned. This consists of an MSISDN, IMSI, SIM, SimImsiMap, HlrServiceProfile and an MsisdnImsiProfileAssociation. For the MAP messages, in the IMS network, this consists of an MSISDN only.

  If a full subscriber profile is absent and/or the Routing functionality is deactivated then the SDM will return the following error "MAP Unknown Subscriber".

Main Routing Criteria

The Routing logic is triggered when the Tekelec ngHLR receives a MAP request. Messages are routed based on the following configurable criteria:

- Originating network - Logic for routing the MAP messages is based on the originating network.
  - HPLMN versus non-HPLMN. To determine this, the Tekelec ngHLR tries to find a match between the SCCP calling party address and the pre-configured HPLMN prefixes (defined in the Tekelec ngHLR's HPLMN entity).

- Exceptions - An Originating SMS-GMSC exception list can be configured in the Tekelec ngHLR. This list is interpreted as a list of SMS-GMSC address prefixes.

  Note: Exceptions only apply to MT-SMS messages.

  - For the MT-SMS Relay functionality, the SCCP CgPA is compared to the SMS-GMSC exception list. The CgPA is normalized (from national to international by adding the country code) prior to comparison.
  - For the MT-SMS Redirect functionality, it is the SC (Service Center) address that is compared to the SMS-GMSC exception list. The SC address is normalized (from national to international by adding the country code) prior to comparison. In the case where a match is found, the Tekelec ngHLR handles MT-SMS requests as per the standard MT-SMS process.

- Routing Trigger - Never, Always, When roaming out of HPLMN, When SIP registered, When SIP registered or roaming out of HPLMN, When in the HPLMN, When SIP registered or in the HPLMN.
- Destination network - Logic for MAP routing is based on the destination network. The Tekelec ngHLR compares the address of the MSC with which the subscriber is currently registered with and tries to find a match with the pre-configured HPLMN prefixes (defined in the Tekelec ngHLR's HPLMN entity).
- Routing type - The Tekelec ngHLR routes the MAP messages based on the configured routing type (Redirect or Relay) defined for each Routing Template.

  Note: For MAP messages sent from other foreign Originator nodes to subscribers registered in a VPLMN in international roaming, the home routing is not applied since the foreign network is the one responsible to handle the termination.

SRI MT-SMS Routing

The Tekelec ngHLR can follow the standard MT-SMS processing behavior by responding to a MAP SRI-for-SM message from the Originator SMS-GMSC by returning a MAP SRI-for-SM Ack message with the IMSI and current MSC address where the subscriber is roaming (currently registered).

However, with the Flexible MT-SMS Rerouting feature, the Tekelec ngHLR can also reroute MAP SRI-for-SM messages as follows:

- MT-SMS Redirect behavior: the Tekelec ngHLR responds to MAP SRI-for-SM messages from the Originator SMS-GMSC by returning a MAP SRI-for-SM Ack message with the default or subscriber IMSI and a configured SMS Router Gt.
- MT-SMS Relay behavior: the Tekelec ngHLR relays the MAP SRI-for-SM messages from the Originator SMS-GMSC to a configurable SMS Router, which in turn responds to the MAP SRI-for-SM request by sending an SRI-for-SM Ack message with the default or subscriber IMSI and a configured SMS Router Gt.

Note: When redirecting a MAP SRI MT-SMS message for a subscriber for which the IMSI is unknown by the Tekelec ngHLR (i.e., subscriber is not registered, subscriber does not have a full subscriber profile provisioned in the Tekelec ngHLR (only MSISDN(s)), the Tekelec ngHLR includes in the SRI MT-SMS Ack message the subscriber IMSI provisioned in the IMSIForRedirectRouting table. If no subscriber IMSI is provisioned in the IMSIForRedirectRouting table for the MSISDN, the Tekelec ngHLR returns a default IMSI, as defined in the SipTasGt (when TAS registered) or DestinationRouter tables. To ensure that the MAP Forward SM message includes a proper IMSI that identifies the subscriber correctly, the Network Operator must provision a subscriber IMSI in the IMSIForRedirectRouting table. This IMSIForRedirectRouting table allows the Network Operator to provision subscriber IMSIs per MSISDNs, as opposed to a default IMSI per routing template, making sure the IMSI is unique for each MSISDN.

MT SMS Routing Template Process

Note: If no full subscriber profile present (only the MSISDN table is populated), the roaming status of the subscriber is unknown. In this case, triggers such as in/out of HPLMN are not relevant and are not used.

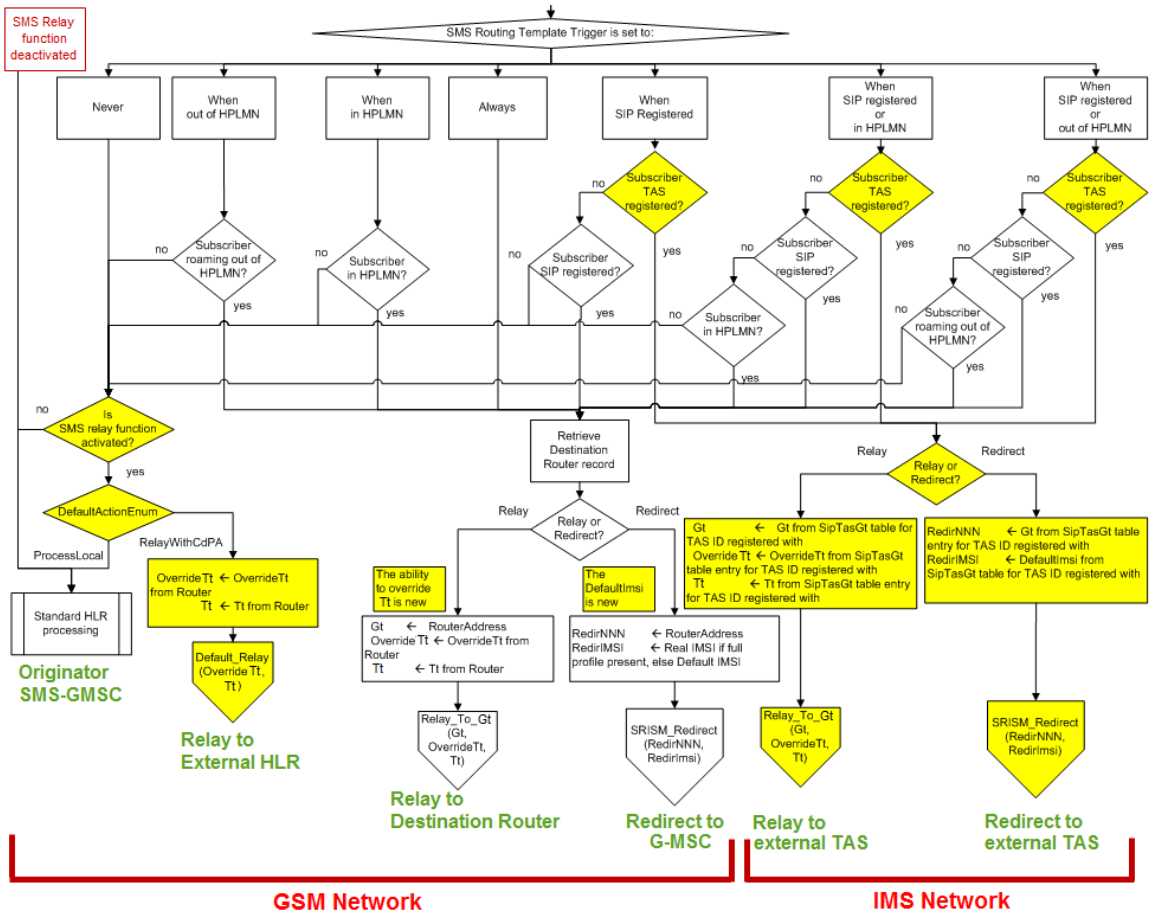


Table 24: Process Routing Template for MT SMS

MT SMS Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
Never	SMS relay activated	Default Action - Relay with CdPA	Default Relay with CdPA process	Relay MT SMS (OverrideTt, Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-	Responds to MT SMS with	G-MSC	GSM

MT SMS Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
			standard HLR process	SMS-Ack (IMSI, current MSC)		
	SMS relay not activated	Default Action - Process locally	Process locally-standard HLR process	Responds to MT SMS with SMS-Ack (IMSI, current MSC)	G-MSC	GSM
When out of HPLMN	Subscriber roaming out of HPLMN	Relay	Relay Process	Relay MT SMS (Gt, OverrideTt, Tt)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect Process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber roaming in HPLMN	Default Action - Relay with CdPA	Default Relay with CdPA process	Relay MT SMS (OverrideTt, Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard HLR process	Responds to MT SMS with SMS-Ack (IMSI, current MSC)	MSC/VLR	GSM
When in HPLMN	Subscriber roaming in HPLMN	Relay	Relay Process	Relay MT SMS (Gt, OverrideTt, Tt)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect Process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber roaming out of HPLMN	Default Action - Relay with CdPA	Default Relay with	Relay MT SMS (OverrideTt, Tt)	External HLR	GSM

MT SMS Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
			CdPA process			
		Default Action - Process locally	Process locally-standard HLR process	Responds to MT SMS with SMS-Ack (IMSI, current MSC)	MSC/VLR	GSM
Always		Relay	Relay process	Relay MT SMS (Gt, OverrideTt, Tt)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
When SIP Registered	Subscriber TAS registered	Relay	Relay process	Relay MT SMS (GT, OverrideTt, Tt)	External TAS	IMS
		Redirect	Redirect process	Redirect MT SMS (REDIRNNN, REDIRIMSI)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay MT SMS (Gt, OverrideTt, Tt)	MSC/VLR	GSM
		Redirect	Redirect process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber not TAS registered Subscriber not SIP registered	Default Action - Relay with CdPA	Default Relay with CdPA process	Relay MT SMS (OverrideTt, Tt)	External HLR	GSM

MT SMS Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
		Default Action - Process locally	Process locally-standard HLR process	Responds to MT SMS with SMS-Ack (IMSI, current MSC)	MSC/VLR	GSM
When SIP Registered or in HPLMN	Subscriber TAS registered	Relay	Relay process	Relay MT SMS (GT, OverrideTT, TT)	External TAS	IMS
		Redirect	Redirect process	Redirect MT SMS (REDIRNNN, REDIRIMSI)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay MT SMS (Gt, OverrideTt, Tt)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber roaming in HPLMN	Relay	Relay process	Relay MT SMS (GT, OverrideTT, TT)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber roaming out of HPLMN	Default Action - Relay with CdPA	Default Relay with CdPA process	Relay MT SMS (OverrideTt, Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard	Responds to MT SMS with	MSC/VLR	GSM

MT SMS Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
			HLR process	SMS-Ack (IMSI, current MSC)		
When SIP Registered or out of HPLMN	Subscriber TAS registered	Relay	Relay process	Relay MT SMS (GT, OverrideTt, Tt)	External TAS	IMS
		Redirect	Redirect process	Redirect MT SMS (REDIRNNN, REDIRIMSI)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay MT SMS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber roaming out of HPLMN	Relay	Relay process	Relay MT SMS (GT, OverrideTT, TT)	Destination Router (as configured in RouterAddress	GSM
		Redirect	Redirect process	Redirect MT SMS (RedirNNN, RedirIMSI)	MSC/VLR	GSM
	Subscriber roaming in HPLMN	Default Action - Relay with CdPA	Default Relay with CdPA process	Relay MT SMS (OverrideTt, Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard HLR process	Responds to MT SMS with SMS-Ack (IMSI, current MSC)	MSC/VLR	GSM

Standard MT-SMS processing

The system already has a default MT-SMS Routing Template and Destination Router entry configured. The default MT-SMS Routing Template is identified by the TemplateName or TemplateId parameters, which are set to 'Not Defined' and 0 correspondingly. By default, all subscriber profiles are assigned to the 'Not Defined' MT-SMS Routing Template.

The Tekelec ngHLR performs the standard MT-SMS processing in the following scenarios:

- Scenario 1:
  - The MT-SMS Routing functionality is deactivated (HlrConfig's SmsRouting parameter set to 0).
- Scenario 2:
  - The MT-SMS Routing functionality is activated (HlrConfig's SmsRouting parameter is set to 1).
  - The subscriber's MSISDN is unknown (not provisioned in the Tekelec ngHLR's database)
- Scenario 3:
  - The MT-SMS Routing functionality is activated (HlrConfig's SmsRouting parameter is set to 1).
  - The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
  - The subscriber does not have a routing template provisioned in the database (the SmsTemplateId='NotDefined' (0) in both the SubscriberProfile and MSISDN tables).

    Note: If the SmsTemplateId is set to 'Not Defined' (0) in the MSISDN [] entity, the Tekelec ngHLR considers that the subscriber is not associated to any routing template. The Tekelec ngHLR then verifies the SmsTemplateID value provisioned in the HlrServiceProfile. If the value in the HlrServiceProfile is 'Not Defined' (0) the Tekelec ngHLR continues processing the message with the standard MT-SMS process.
- Scenario 4:
  - The MT-SMS Routing functionality is activated (HlrConfig's SmsRouting parameter is set to 1).
  - The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
  - The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value).
  - There is no full subscriber profile for the subscriber.

    Note: A full subscriber profile consists of at least an MSISDN, an IMSI, and a SIM , as well as a SimImsiMap, an HlrServiceProfile, and a MsisdnImsiProfileAssociation. For subscribers registered in the IMS network, only an MSISDN is required with an associated SMS Routing Template.
  - The MT-SMS Relay functionality is deactivated (HlrConfig's SmsRelay parameter is set to 0).
- Scenario 5:
  - The MT-SMS Routing functionality is activated (HlrConfig's SmsRouting parameter is set to 1).
  - The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
  - The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value).
  - There is a full subscriber profile provisioned for the subscriber in the Tekelec ngHLR.

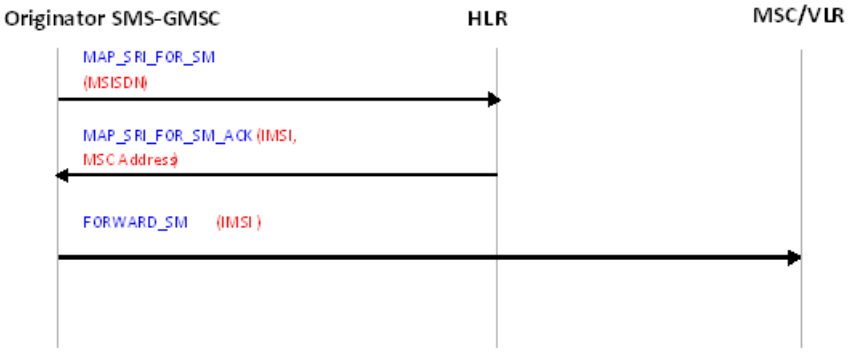
- The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) matches one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

- Scenario 6:
  - The MT-SMS Routing and MT-SMS Relay functionalities are both activated (HlrConfig's SmsRouting and SmsRelay parameters are both set to 1).
  - The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
  - The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value).
  - The subscriber has a full subscriber profile provisioned in the Tekelec ngHLR.
  - The routing template provisioned for the subscriber's MSISDN is set as follows:
    - The routing trigger is set to a value 'Never' or any other value than "Never" and is not successfully met.
    - The default action is set to 'ProcessLocal'.
    - The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) does not match one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

Standard MT-SMS flow is as follows:

- The Tekelec ngHLR receives a request from the Originator SMS-GMSC.
- The Tekelec ngHLR replies with an acknowledgment that includes an IMSI and an MSC address where the subscriber is currently registered.
- The SM is forwarded to the MSC.

Figure 34: Call flow for Standard MT-SMS Routing



Flexible MT-SMS Rerouting

The Flexible MT-SMS Rerouting feature allows the Network Operator to configure the Tekelec ngHLR to reroute the MT-SMS request sent by an Originator SMS-GMSC. The Tekelec ngHLR supports two types of flexible MT-SMS rerouting functionalities:

1. MT-SMS Redirect
2. MT-SMS Relay

There are many benefits in selecting the MT-SMS Rerouting functionalities for handling MT-SMS messages, such as:

- The possibility of having the MT-SMS rerouted to an Instant Message (IM) or to an IP SMS.
- Added control of MT-SMS routing even while the subscriber is roaming.
- Support of the following MT-SMS services to enhance security for MT-SMS originated from foreign networks:
  - SMS Spam filtering and virus checking
  - SMS mailbox/archives
  - Insert advertisement
  - SMS forking
  - Real-time SMS billing

MT-SMS Relay

The Network Operator can configure the Tekelec ngHLR to relay MT-SMS requests from the Originator SMS-GMSC to the Home Network's Destination Router (SMS Router), which in turn responds to the MAP SRI-for-SM message by sending an acknowledgment that contains an IMSI and a configured SMS Router Gt address.

The messages can be relayed to:

- Destination Router (in the GSM network)
- External HLR (in the GSM network)
- External TAS (in the IMS network)

MT-SMS Relay Flow to the Destination Router in the GSM Network

The Tekelec ngHLR performs the MT-SMS Relay to Destination Router processing in the following scenario:

- The MT-SMS Routing and MT-SMS Relay functionalities are both activated (HlrConfig's SmsRouting and SmsRelay parameters are both set to 1).
- The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
- The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value that refers to an entry in the RoutingTemplate table).
- The subscriber has a full subscriber profile provisioned in the Tekelec ngHLR.
- The routing template provisioned for the subscriber's MSISDN is set as follows:
  - The routing trigger is set to a value other than 'Never' and is successfully met.
  - The subscriber is not TAS registered.
  - The routing type is set to 'Relay'.
  - The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) doesn't match one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

The MT-SMS Relay flow to the Destination Router (SMS Router) in the GSM Network is as follows:

- The Tekelec ngHLR receives a MAP SRI-for-SM request from the originator SMS-GMSC. The SDM looks up the MSISDN in the database, its volatile data and the routing template associated to it.
- Based on the information gathered in the database, the Tekelec ngHLR relays the MAP SRI-for-SM message to the correct SMS Router, by including the Gt and Tt as per configured in the DestinationRouter table.

- The SMS Router replies to the originator SMS-GMSC with a MAP SRI-for-SM-Ack including the IMSI and SMS Router Gt.
- The Originator SMS-GMSC forwards the IMSI and the SMS Router Gt address to the SMS Router.
- The SMS Router forwards the SM with the IMSI and the MSC Gt to the MSC where the subscriber is roaming (currently registered)
- The MSC sends back an acknowledgment to the SMS Router.
- The SMS Router forwards the acknowledgment to the Originator SMS-GMSC.

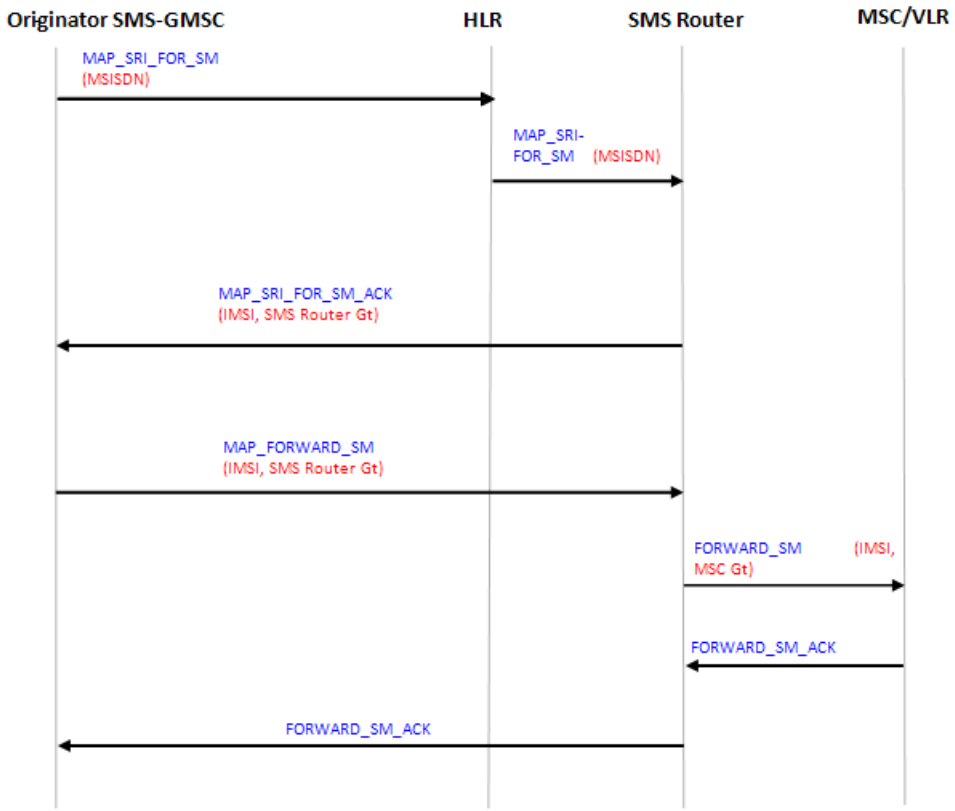


Figure 35: Call flow for MT-SMS Relay to the Destination Router within the GSM Network

MT-SMS Relay flow to an external HLR in the GSM Network

The Tekelec ngHLR performs the MT-SMS Relay to an external HLR (aka Default Relay) processing in the following scenario:

- The MT-SMS Routing and MT-SMS Relay functionalities are both activated (HlrConfig's SmsRouting and SmsRelay parameters are both set to 1).
- The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
- The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value that refers to an entry in the RoutingTemplate table).
- The subscriber has a full subscriber profile provisioned in the Tekelec ngHLR.
- The routing template provisioned for the subscriber's MSISDN is set as follows:
  - The routing trigger is set to 'Never' or to any other value and is not successfully met.

- The default Action is set to 'RelayWithCdPA'.
- The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) doesn't match one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

The MT-SMS Relay flow to an external HLR in the GSM Network is as follows:

- The Tekelec ngHLR in the SDM receives a MAP SRI-for-SM request from the originator SMS-GMSC. The SDM looks up the MSISDN in the database, its volatile data and the routing template associated to it.
- Based on the information gathered in the database, the Tekelec ngHLR relays the MAP SRI-for-SM message to the correct external HLR, by including the same Gt as received (using the same CdPA) and changing the Tt as per configured in the DestinationRouter table.
- The external HLR replies to the originator SMS-GMSC. It sends a MAP SRI-for-SM-Ack message, which includes the network node number and the IMSI of the subscriber.
- The originator SMS-GMSC then forwards the message to the MSC.

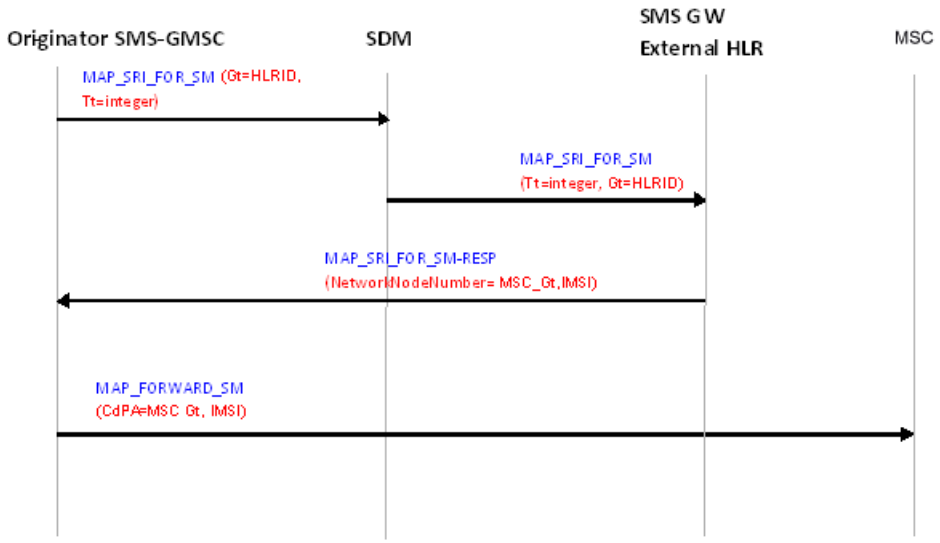


Figure 36: Call flow for MT-SMS Relay to the external HLR within the GSM Network

Alert Service Center feature to build CdPA (Relay to GSM Network)

The Hlr Alert Service Center processing saves the SCCP's CdPA of the SRI-for-SM to be reused as the CdPA for when the Alert Service Center message will need to be sent. In the context of the MT-SMS Relay, this is problematic since it is the SMS-Relay address that sends the MAP SRI-for-SM instead of the ServiceCenter.

When executing the MT-SMS Relay functionality, the Tekelec ngHLR cannot get the correct address of the Alert Service Center from the SCCP header. It must retrieve the Alert Service Center's address from the MAP header instead. This feature permits the Alert Service Center generation to use the ServiceCenter Address to rebuild the CdPA from the ServiceCenter Address.

This feature can be activated/deactivated by the Network Operator dynamically from the WebCI and CLI, by configuring the 'AlertSCBuildCdPA' attribute in the Tekelec ngHLR's HlrConfig.

It is very important that this feature remains activated if the 'SmsRelay' functionality is activated. For further details on the AlertSCBuildCdPA attribute, refer to the "HLR Configuration" section of the *SDM System Configuration - Reference Manual*. For instructions on how to configure the Alert Service Center feature to build CdPA, refer to the "Viewing activation status of HLR features and activating/deactivating them individually" section of the *SDM System Configuration - User Guide*.

MT-SMS Relay flow to an external TAS in the IMS Network

The Tekelec ngHLR performs the MT-SMS Relay to an external TAS processing in the following scenario:

- The MT-SMS Routing and MT-SMS Relay functionalities are both activated (HlrConfig's SmsRouting and SmsRelay parameters are both set to 1).
- The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
- The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value that refers to an entry in the RoutingTemplate table).
- The subscriber is TAS registered.
- The subscriber has a full subscriber profile provisioned in the Tekelec ngHLR.

  Note: To route MT-SMS messages for a subscriber that is TAS registered, a full subscriber profile only consists in the provisioned MSISDNs.

- The routing template provisioned for the subscriber's MSISDN is set as follows:
  - The routing trigger is set to one of the following values and is successfully met:
    - When SIP Registered
    - When SIP Registered or in HPLMN
    - When SIP Registered or out of HPLMN
  - The routing type is set to 'Relay'
  - The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) doesn't match one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

The MT-SMS Relay flow to an external TAS in the IMS Network is as follows:

- The Tekelec ngHLR in the SDM receives a MAP SRI-for-SM request from the originator SMS-GMSC. The SDM looks up the MSISDN in the database, its volatile data and registration bindings and the routing template associated to the MSISDN. If the subscriber's registration bindings have a TasId with a value other than 0 then it is TAS registered. It is an IMS subscriber and the message will be relayed to an external TAS.
- Based on the information gathered in the database, the Tekelec ngHLR relays the MAP SRI-for-SM message to the correct external TAS, by including the Gt and Tt as per configured in the SipTasGt table.

  Note: If the value of the override Tt in the SipTasGt table is 0 then the Tt value is not changed. If the override Tt value is 1 then the Tt is overwritten.

- The external TAS replies to the originator SMS-GMSC. It sends back a MAP SRI-for-SM Ack. This message contains the network node number and an IMSI.
- The originator SMS-GMSC then forwards the message to the external TAS.

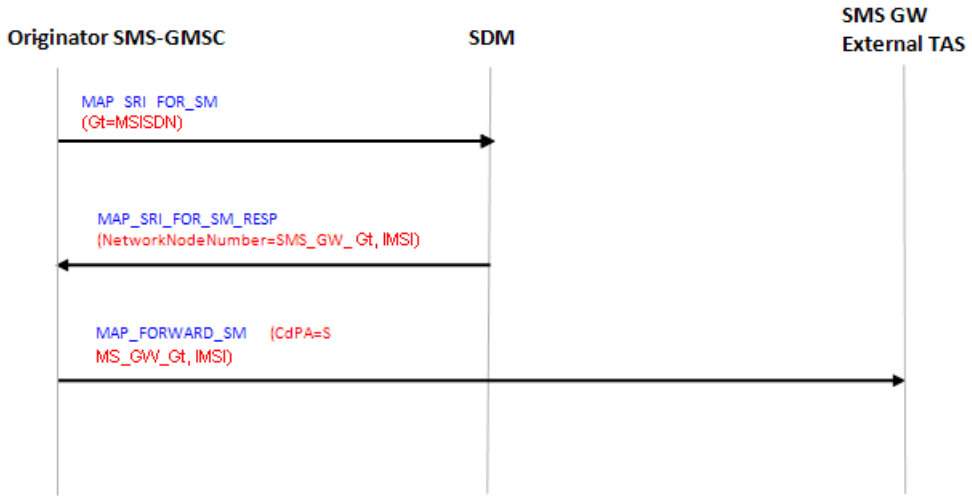


Figure 37: Call flow for MT-SMS Relay to the external TAS within the IMS Network

MT-SMS Redirect

The Network Operator can configure the Tekelec ngHLR to redirect MT-SMS requests to the Home Network's Destination Router (SMS Router), by returning back to the Originator SMS-GMSC the Gt address of that SMS Router. The message then gets forwarded to the SMS Router, which forwards the SM to the current MSC/VLR.

The message can be redirected to:

- MSC/VLR (in the GSM network)
- External TAS (in the IMS network)

MT-SMS Redirect flow to the MSC/VLR in the GSM Network

The Tekelec ngHLR performs the MT-SMS Redirect to MSC/VLR processing in the following scenario:

- The MT-SMS Routing functionality is activated (HlrConfig's SmsRouting attribute is set to 1).
- The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
- The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value that refers to an entry in the RoutingTemplate table).
- The subscriber has a full subscriber profile provisioned in the Tekelec ngHLR.
- The routing template provisioned for the subscriber's MSISDN is set as follows:
  - The routing trigger is set to a value other than 'Never' and is successfully met.
  - The subscriber is not TAS registered.
  - The routing type is set to 'Redirect'.
  - The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) doesn't match one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

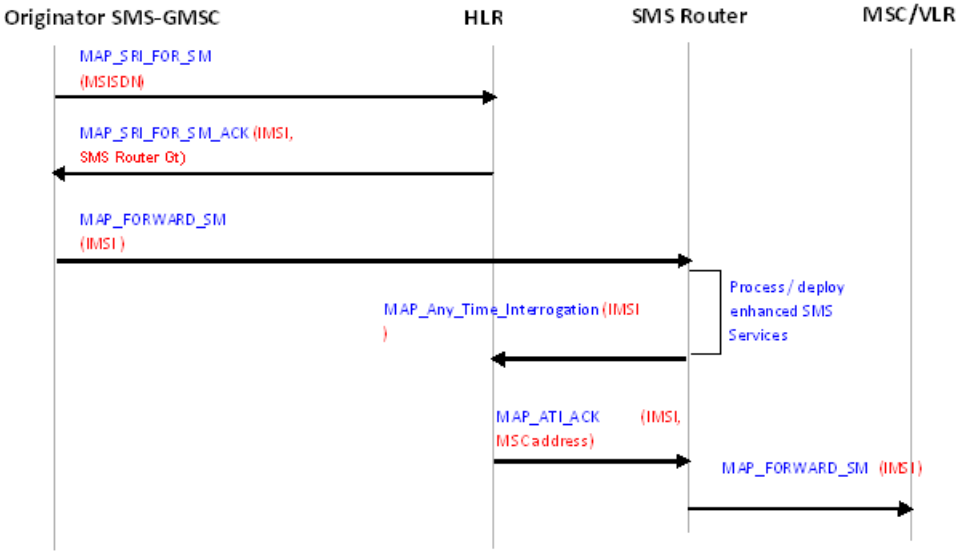
The MT-SMS Redirect flow is as follows:

- The Tekelec ngHLR receives a request from the originator SMS-GMSC.The Tekelec ngHLR looks up the MSISDN in the database, its volatile data and registration bindings and the routing template associated to it.
- Based on the information gathered in the database, the Tekelec ngHLR redirects the message by replying to the SMS-GMSC with a MAP MT-SMS Ack, which includes a subscriber IMSI or default IMSI and a SMS Router Gt address.

  Note: When choosing the IMSI to return, the Tekelec ngHLR first looks into the IMSIForRedirectRouting table to verify if a subscriber IMSI has been provisioned for the MSISDN. If no subscriber is provisioned in this table, the Tekelec ngHLR sends back the default IMSI configured in the routing template's Destination Router table.

- The SMS-GMSC then forwards the MT-SMS message to an SMS Router in the Home PLMN of the destination subscriber, based on the SMS Router Gt address received from the Tekelec ngHLR.
- The SMS Router may need to query the Tekelec ngHLR using:
  - An Any_Time_Interrregation Request.
  - A SRI_SM (if the SMS Router is able to match the IMSI to MSISDN). The Tekelec ngHLR ensures that the MSC address is contained in the ATI-ack message.
- The SMS Router can then forward the SM to the current MSC (where the subscriber is currently registered).

Figure 38: Call flow for MT-SMS Redirect to the MSC/VLR (in the GSM network)



MT-SMS Redirect flow to the external TAS in the IMS Network

The Tekelec ngHLR performs the MT-SMS Redirect to external TAS processing in the following scenario:

- The MT-SMS Routing functionality is activated (HlrConfig's SmsRouting attribute is set to 1).
- The MSISDN received in the MT-SMS message is provisioned in the Tekelec ngHLR.
- The MSISDN has a routing template provisioned (SmsTemplateId attribute in the MSISDN[] or in the SubscriberProfile table is set to a supported value that refers to an entry in the RoutingTemplate table).

- The subscriber has a full subscriber profile provisioned in the Tekelec ngHLR.

  Note: For a TAS registered subscriber, simply provisioned MSISDNs consist of a full subscriber profile in the Tekelec ngHLR.

- The routing template provisioned for the subscriber's MSISDN is set as follows:
  - The routing trigger is set to one of the following values and is successfully met:
    - When SIP registered
    - When SIP registered or in HPLMN
    - When SIP registered or out of HPLMN
  - The subscriber is TAS registered.
  - The routing type is set to 'Redirect'.
  - The Normalized CgPA (for Relay routing type) or the Normalized ServiceCenter address (for Redirect routing type) doesn't match one of the SMS-GMSC Exception router prefixes configured for the subscriber's routing template.

The MT-SMS Redirect flow to the external TAS in the IMS Network is as follows:

- The Tekelec ngHLR receives a request from the originator SMS-GMSC. The Tekelec ngHLR looks up the MSISDN in the database, its volatile data and registration bindings and the routing template associated to it.
- Based on the information gathered in the database, the Tekelec ngHLR redirects the message by replying to the SMS-GMSC with a MAP MT-SMS Ack, which includes a subscriber IMSI or default IMSI and a Network Node Number, which is the TAS Gt as per configured in the SipTasGt table.

  Note: When choosing the IMSI to return, the Tekelec ngHLR first looks into the IMSIForRedirectRouting table to verify if a subscriber IMSI has been provisioned for the MSISDN. If no subscriber is provisioned in this table, the Tekelec ngHLR sends back the default IMSI configured in the SipTasGt table for the subscriber's TasId (the TasId is found based on the subscriber's registration bindings).

- The SMS-GMSC then forwards the MT-SMS message to the external TAS.

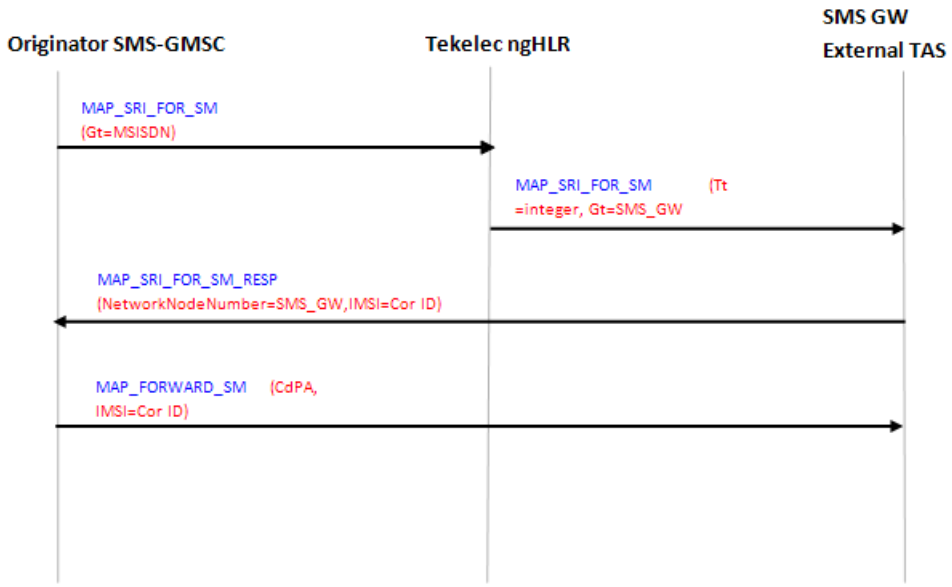


Figure 39: Call flow for MT-SMS Redirect to the external TAS within the IMS Network

SRI/SRI-LCS Routing

The Tekelec ngHLR can follow the standard MAP SRI and MAP SRI FOR LCS processing behaviors as follows:

- Upon receiving a MAP SRI message, the ngHLR responds to the G-MSC with a MAP SRI ACK message, which includes the IMSI and the current MSC address where the subscriber is roaming (currently registered).
- Upon receiving a MAP SRI FOR LCS message, the ngHLR responds to the G-MLC with a MAP SRI FOR LCS ACK message, which includes the IMSI or MSISDN and the Network Node Number.

However, with the SRI and SRI-LCS Routing functionalities, the Tekelec ngHLR can route MAP SRI and MAP SRI FOR LCS messages as follows:

- SRI Routing:
  - SRI Redirect behavior: the Tekelec ngHLR responds to MAP SRI messages from the Originator G-MSC by returning a MAP SRI Ack message with the IMSI and a configured Destination Router Gt.
  - SRI Relay behavior: the Tekelec ngHLR relays the MAP SRI messages from the Originator G-MSC to a configurable Destination Router, which in turn responds to the MAP SRI message by sending a MAP SRI Ack message with the IMSI and a configured Router Gt.
- SRI-LCS Routing:
  - SRI-LCS Redirect behavior: the Tekelec ngHLR responds to MAP SRI FOR LCS messages from the G-MLC by returning a MAP SRI FOR LCS ACK message with the IMSI or MSISDN, the Network Node Number and a configured Destination Router Gt. This allows the G-MLC to then be able to forward the MAP SRI FOR LCS message to the correct Destination Router.
  - SRI-LCS Relay behavior: the Tekelec ngHLR relays the MAP SRI FOR LCS messages from the G-MLC to a configurable Destination Router, which in turn responds to the MAP SRI FOR LCS message by sending a MAP SRI FOR LCS ACK message with the IMSI or MSISDN.

The Tekelec ngHLR can be configured to:

- Relay MAP SRI/SRI-LCS messages to:
  - Destination Router (in the GSM Network)
  - External HLR (in the GSM Network)
  - External TAS (in the IMS Network)

- Redirect MAP SRI/SRI-LCS messages to:
  - G-MSC/G-MLC (in the GSM Network)
  - External TAS (in the IMS Network)

The sections below describe each SRI/SRI-LCS Routing processing option in details.

SRI/SRI-LCS Routing Template Process

Table 25: Process Routing Template for SRI /SRI-LCS shows the behavior of the Tekelec ngHLR based on the Routing Template configuration.

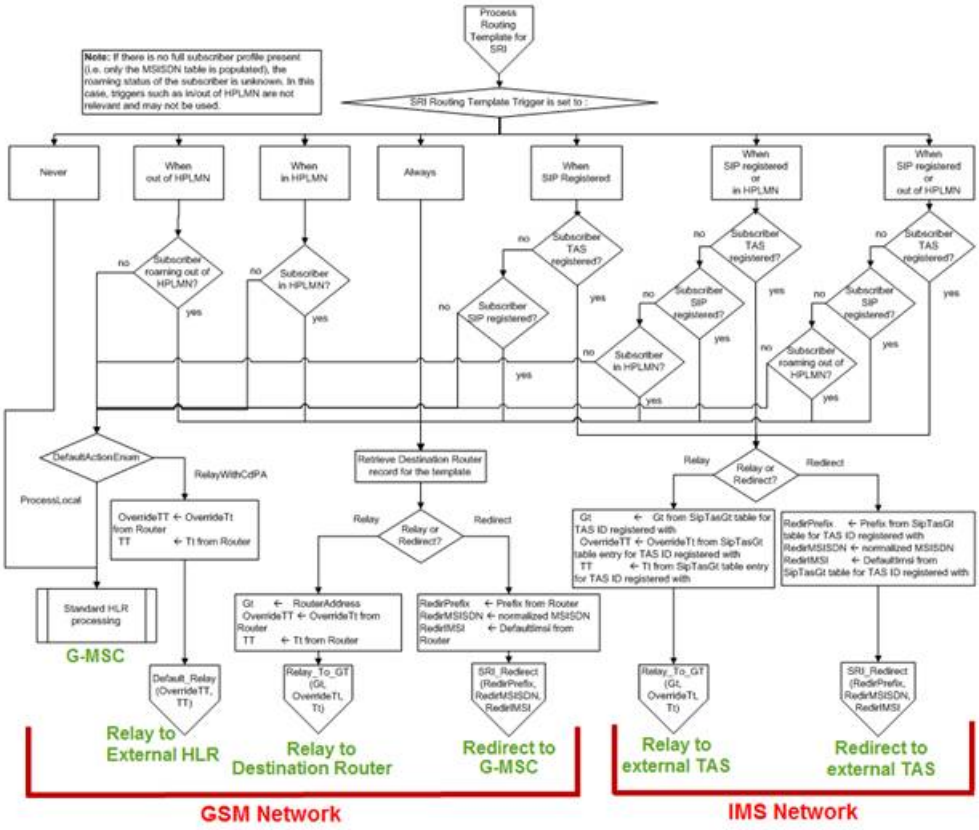


Figure 40: SRI message routing in the Tekelec ngHLR

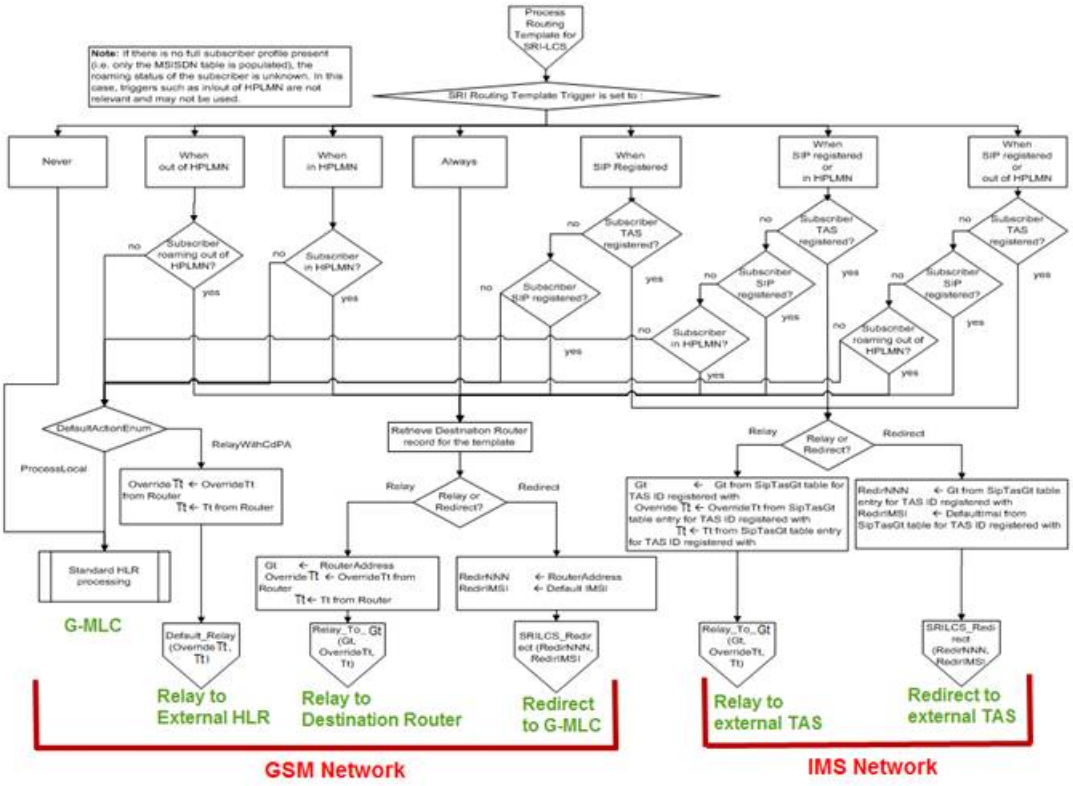


Figure 41: SRI-LCS message routing in the Tekelec ngHLR

Table 25: Process Routing Template for SRI /SRI-LCS

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
Never		Relay/ Redirect	Process locally-standard HLR process	Responds to SRI with SRI-Ack (IMSI, current MSC) Or Responds to SRI-LCS with MAP SRI for LCS-Ack (IMSI/MSISDN, Network Node Number)	G-MSC Or G-MLC	GSM

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
When out of HPLMN	Subscriber roaming out of HPLMN	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	G-MSC Or G-MLC	GSM
	Subscriber roaming in HPLMN	Default Action - Process locally	Process locally-standard HLR process	Responds to SRI with SRI-Ack (IMSI, current MSC) Or Responds to SRI-LCS with MAP SRI for LCS-Ack (IMSI/MSISDN, Network Node Number)	G-MSC Or G-MLC	GSM
		Default Action - Relay with CdPA	Default Relay with CdPA process	Relay SRI/ SRI-LCS (OverrideTt,Tt)	External HLR	GSM
When in HPLMN	Subscriber roaming in HPLMN	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or	G-MSC Or G-MLC	GSM

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
				Redirect SRI-LCS (RedirNNN, RedirIMSI)		
	Subscriber roaming out of HPLMN	Default Action - Process locally	Process locally-standard HLR process	Responds to SRI with SRI-Ack (IMSI, current MSC) Or Responds to SRI-LCS with MAP SRI for LCS-Ack (IMSI/MSISDN, Network Node Number)	G-MSC Or G-MLC	GSM
		Default Action - Relay with CdPA	Default Relay with CdPA process	Relay SRI/ SRI-LCS (OverrideTt,Tt)	External HLR	GSM
Always		Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	G-MSC Or G-MLC	GSM
When SIP Registered	Subscriber TAS registered	Relay	Relay process	Relay SRI/SRI-LCS (Gt, OverrideTt,Tt)	External TAS	IMS
		Redirect	Redirect process	Redirect SRI (RedirPrefix,	External TAS	IMS

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
				RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)		
	Subscriber SIP registered	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	G-MSC Or G-MLC	GSM
	Subscriber not TAS registered Subscriber not SIP registered	Default Action - Process locally	Process locally-standard HLR process	Responds to SRI with SRI-Ack (IMSI, current MSC) Or Responds to SRI-LCS with MAP SRI for LCS-Ack (IMSI/MSISDN, Network Node Number)	G-MSC Or G-MLC	GSM
		Default Action - Relay with CdPA	Default Relay with CdPA process	Relay SRI/SRI-LCS (OverrideTt,Tt)	External HLR	GSM
When SIP Registered or in HPLMN	Subscriber TAS registered	Relay	Relay process	Relay SRI/SRI-LCS	External TAS	IMS

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
				(Gt, OverrideTt,Tt)		
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	G-MSC	GSM
	Subscriber roaming in HPLMN	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	G-MSC Or G-MLC	GSM

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
	Subscriber roaming out of HPLMN	Default Action - Process locally	Process locally-standard HLR process	Responds to SRI with SRI-Ack (IMSI, current MSC Or Responds to SRI-LCS with MAP SRI for LCS-Ack (IMSI/MSISDN, Network Node Number)	G-MSC Or G-MLC	GSM
		Default Action - Relay with CdPA	Default Relay with CdPA process	Relay SRI/SRI-LCS (OverrideTt,Tt)	External HLR	GSM
When SIP Registered or out of HPLMN	Subscriber TAS registered	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	External TAS	IMS
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS	G-MSC Or G-MLC	GSM

Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
				(RedirNNN, RedirIMSI)		
	Subscriber roaming out of HPLMN	Relay	Relay process	Relay SRI/SRI-LCS (Gt,OverrideTt,Tt)	Destination Router (as configured in RouterAddress)	GSM
		Redirect	Redirect process	Redirect SRI (RedirPrefix, RedirMSISDN, RedirIMSI) Or Redirect SRI-LCS (RedirNNN, RedirIMSI)	G-MSC Or G-MLC	GSM
	Subscriber roaming in HPLMN	Default Action - Process locally	Process locally-standard HLR process	Responds to SRI with SRI-Ack (IMSI, current MSC Or Responds to SRI-LCS with MAP SRI for LCS-Ack (IMSI/MSISDN, Network Node Number)	G-MSC Or G-MLC	GSM
		Default Action - Relay with CdPA	Default Relay with CdPA process	Relay SRI/SRI-LCS (OverrideTt,Tt)	External HLR	GSM

SRI/SRI-LCS Standard Process

The Tekelec ngHLR performs the standard SRI/SRI-LCS processing in the following scenarios:

- Scenario 1:
  - The SRI Routing functionality is deactivated (HlrConfig's SriRouting parameter set to 0).
- Scenario 2:
  - The subscriber's MSISDN is unknown (not provisioned in the Tekelec ngHLR's database)

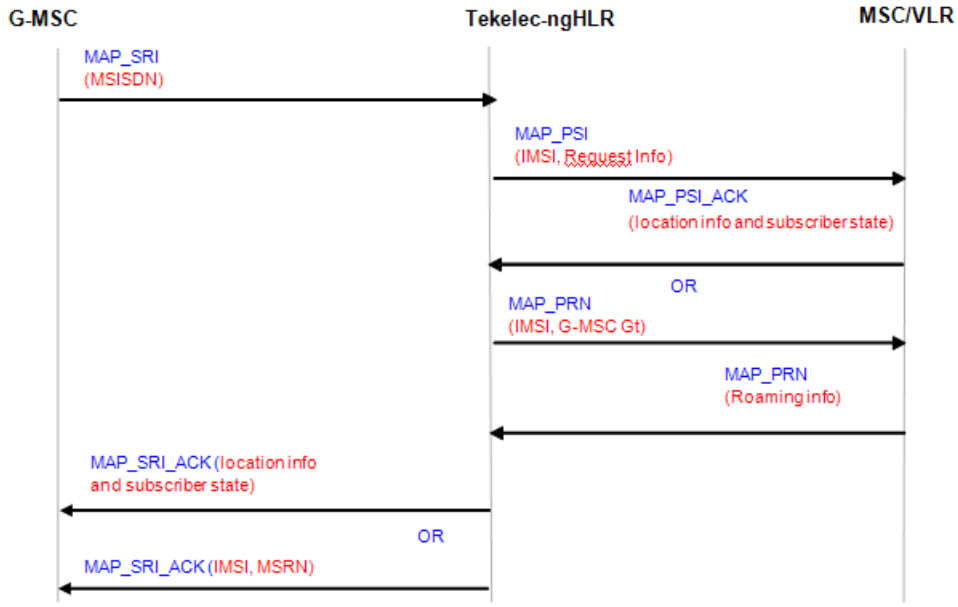
    - The SRI Routing functionality's activation status is set to 'Template Only'.

- Scenario 3:
    - The SRI Routing functionality is activated and set to 'Template Only'.
    - The MSISDN received in the SRI/SRI-LCS message is provisioned in the Tekelec ngHLR.
    - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
- Scenario 4:
    - The SRI Routing functionality is activated (HlrConfig's SriRouting attribute is set to 'Relay', 'Redirect' or 'TemplateOnly').
    - The MSISDN received in the SRI/SRI-LCS message is provisioned in the Tekelec ngHLR.
    - The MSISDN has a routing template provisioned (SriTemplateId attribute in the MSISDN[] entity is set to a supported value that refers to an entry in the RoutingTemplate[] table).
    - The subscriber's MSISDN has a routing template provisioned with a routing trigger set to 'Never'.
- Scenario 5:
    - The SRI Routing functionality is activated (HlrConfig's SriRouting attribute is set to 'Relay', 'Redirect' or 'TemplateOnly').
    - The MSISDN received in the SRI/SRI-LCS message is provisioned in the Tekelec ngHLR.
    - The MSISDN has a routing template provisioned (SriTemplateId attribute in the MSISDN[] entity is set to a supported value that refers to an entry in the RoutingTemplate[] table).
    - The routing template provisioned for the subscriber's MSISDN is set as follows:
        - The routing trigger is set to a value other than 'Never' and is not successfully met.
        - The default action is set to 'ProcessLocal'.

The standard SRI flow is as follows:

- The Tekelec ngHLR receives a request from the G-MSC.
- The Tekelec ngHLR sends either one of the following messages to the MSC/VLR:
    - Provide Subscriber Information (PSI) message: in order to retrieve subscriber data update and status.
    - Provide Roaming Number (PRN): in order to retrieve a roaming number.
- The MSC/VLR replies to the Tekelec ngHLR with a PSI-Ack message including subscriber data status and location information or with a PRN-Ack message including routing info.
- The Tekelec ngHLR sends back a MAP-Ack to the G-MSC with the information retrieved from the MSC/VLR through the PSI or PRN process (i.e. subscriber state and location information or routing information).

Figure 42: Call flow for Standard SRI Routing



Note: The Tekelec ngHLR sending Provide Roaming Number or Provide Subscriber Info depends on if the subscriber has Camel TCSI service and Camel parameter in Send Routing Info request.

The standard SRI-LCS flow is as follows:

- The Tekelec ngHLR receives a request from the G-MLC including the mandatory parameters (IMSI or MSISDN, MLC number).
- The Tekelec ngHLR replies back to the G-MLC with a MAP_SRI_FOR_LCS-ACK message including subscriber identification and the network node number.

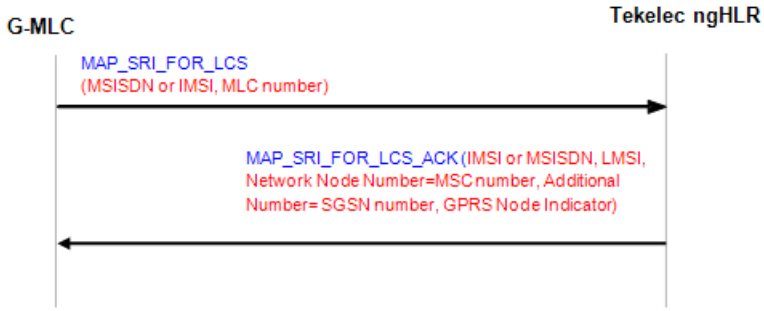


Figure 43: Call flow for Standard SRI-LCS Routing

SRI/SRI-LCS Default Relay with CdPA processing to external HLR

The Tekelec ngHLR performs the Default Relay with CdPA processing to an external HLR in the following cases:

- Scenario 1:
  - The subscriber's MSISDN is unknown by the Tekelec ngHLR (either it is not provisioned in the Tekelec ngHLR's database or the SRI-LCS request includes the IMSI instead of the MSISDN)
  - The SRI Routing functionality is activated and is set to 'Relay' or 'Redirect'

- Scenario 2:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Redirect'
  - The subscriber is not TAS registered
- Scenario 3:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Relay'
  - The subscriber is not TAS registered
- Scenario 4:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate entity)
  - The routing template is set as follows:
    - The routing trigger is not set to 'Never' and is not met.
    - The default action is set to RelayWithCdPA.

The SRI/SRI-LCS Default Relay with CdPA call flows are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS request from the G-MSC/G-MLC
- The Tekelec ngHLR relays the request to the external HLR using the same Gt as the one received in the request, but with a possible different Tt, based on the information configured in the subscriber's routing template DestinationRouter table.
- The external HLR replies to the G-MSC/G-MLC with a MAP_SRI_ACK/MAP_SRI_FOR_LCS_ACK.

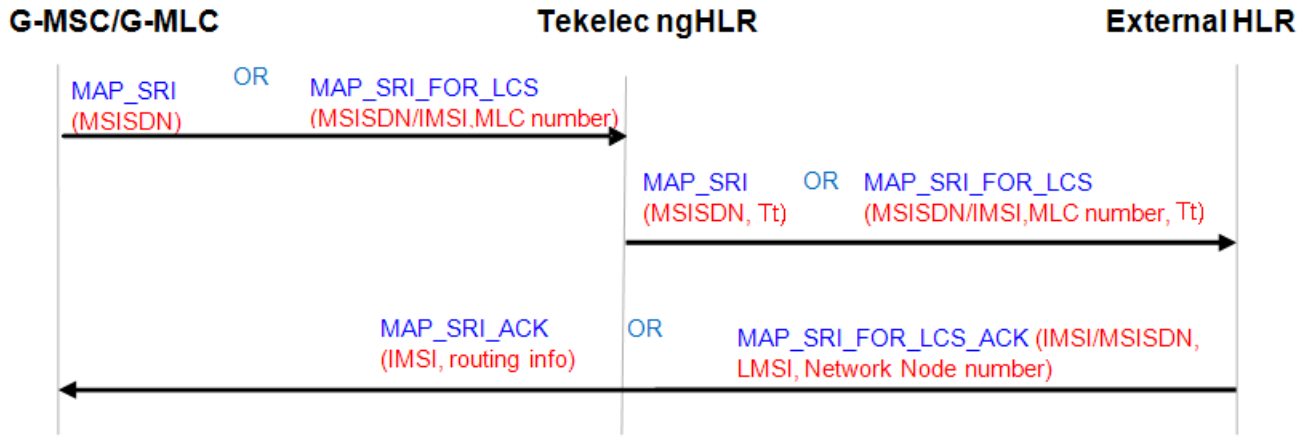


Figure 44: Call flow for SRI/SRI-LCS Default Relay with CdPA to an external HLR within the GSM Network

SRI/SRI-LCS Relay Processing to Destination Router

The Tekelec ngHLR can relay SRI/SRI-LCS messages to one of the Destination Routers defined in the system's Routing Controls (in the DestinationRouter[] entity).

The Tekelec ngHLR performs the Relay processing to a Destination Router in the following scenario:

- The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
- The MSISDN received in the SRI message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
- The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate entity)
- The subscriber is not TAS registered
- The routing template is set as follows:
  - The routing trigger is not set to 'Never' and is successfully met.
  - The routing type is set to 'Relay'.

The SRI/SRI-LCS Relay call flows are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS request from the G-MSC/G-MLC.
- The Tekelec ngHLR relays the request to the Destination Router based on the information configured in the subscriber's routing template DestinationRouter table.
- The Destination Router replies to the G-MSC/G-MLC with a MAP_SRI_ACK/MAP_SRI_FOR_LCS_ACK.

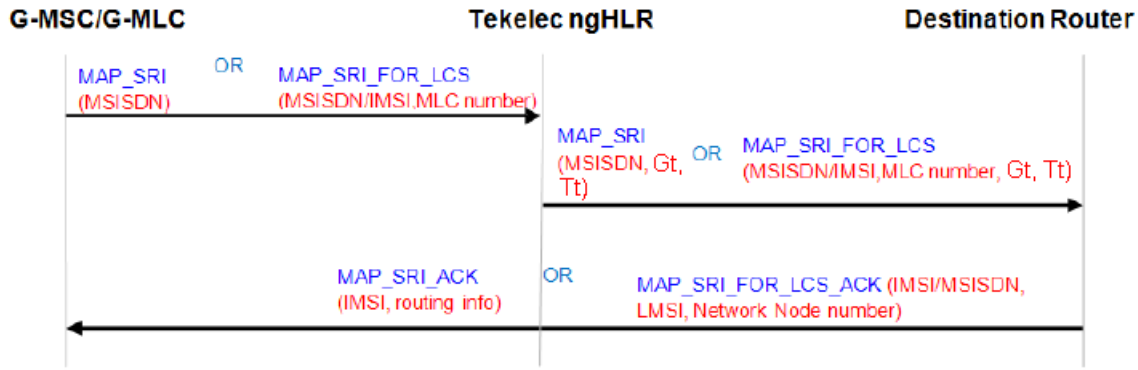


Figure 45: Call flow for SRI/SRI-LCS Relay to a Destination Router within the GSM Network

SRI/SRI-LCS Relay processing to external TAS

The Tekelec ngHLR can relay SRI/SRI-LCS messages to one of the TAS GT defined in the system's SipTasGt[] entity.

The Tekelec ngHLR performs the Relay processing to an external TAS in the following scenarios:

- Scenario 1:
  - The MSISDN received in the SRI message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Relay'
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered
- Scenario 2
  - The MSISDN received in the SRI message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)
  - The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered
  - The routing template is configured as follows:
    - Routing type set to 'Relay'
    - The routing trigger must be set to one of the following values and must be successfully met with the subscriber being TAS registered:
      - 'When SIP Registered'
      - 'When SIP Registered or in HPLMN'
      - 'When SIP Registered or out of HPLMN'

The SRI/SRI-LCS Relay call flows are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS request from the G-MSC/G-MLC
- The Tekelec ngHLR relays the SRI/SRI-LCS request to the external TAS based on the information configured in the SipTasGt table for the TasId stored in the subscriber's registration binding
- The external TAS replies to the G-MSC/G-MLC with a MAP_SRI_ACK/MAP_SRI_FOR_LCS_ACK

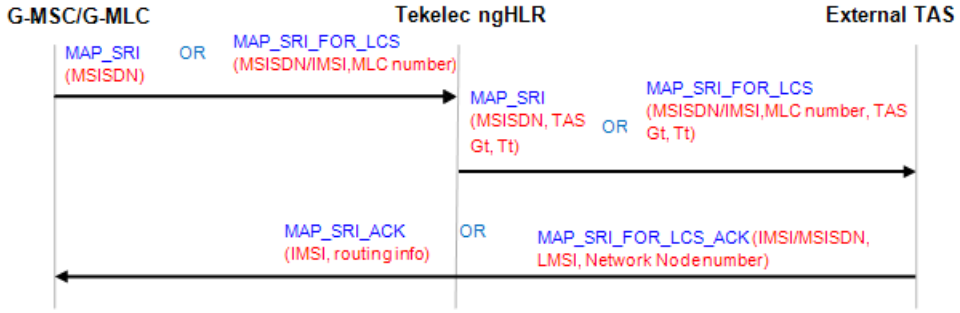


Figure 46: Call flow for SRI/SRI-LCS Relay to the external TAS within the IMS Network

SRI/SRI-LCS Relay

The Network Operator can configure the Tekelec ngHLR to relay SRI/SRI-LCS messages to one of the following nodes, by returning the Tt and/or Gt of the originating node:

- External HLR (in the GSM network)
- Destination Router (in the GSM network)
- External TAS (in the IMS network)

SRI/SRI-LCS Default Relay with CdPA processing to external HLR

The Tekelec ngHLR performs the Default Relay with CdPA processing to an external HLR in the following scenarios:

- Scenario 1:
  - The subscriber's MSISDN is unknown by the Tekelec ngHLR (either it is not provisioned in the Tekelec ngHLR's database or the SRI-LCS request includes the IMSI instead of the MSISDN)
  - The SRI Routing functionality is activated and is set to 'Relay' or 'Redirect'
- Scenario 2:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Redirect'
  - The subscriber is not TAS registered
- Scenario 3:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Relay'

- The subscriber is not TAS registered

- Scenario 4:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate entity)
  - The routing template is set as follows:
    - The routing trigger is set to any other value than 'Never' and is not met.
    - The default action is set to RelayWithCdPA.

The SRI/SRI-LCS Default Relay with CdPA call flows are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS request from the G-MSC/G-MLC
- The Tekelec ngHLR relays the request to the external HLR using the same Gt as the one received in the request, but with a possible different Tt, based on the information configured in the subscriber's routing template DestinationRouter table or in the SipTasGt table. In the scenarios 1,2,3 described above, the Tekelec ngHLR reads the Override Tt and Tt information from the SipTasGt table for the TasId=0 entry. In scenario 4, the Tekelec ngHLR reads the Override Tt and Tt information from the Destination Router table.
- The external HLR replies to the G-MSC/G-MLC with a MAP_SRI_ACK/MAP_SRI_FOR_LCS_ACK.

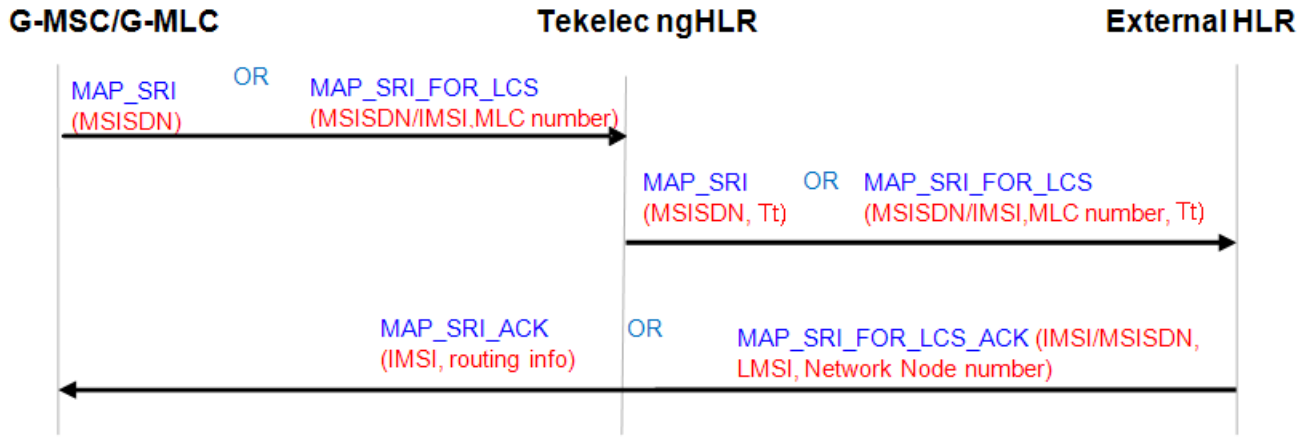


Figure 47: Call flow for SRI/SRI-LCS Default Relay with CdPA to an external HLR within the GSM Network

SRI/SRI-LCS Relay Processing to Destination Router

The Tekelec ngHLR can relay SRI/SRI-LCS messages to one of the Destination Routers defined in the system's Routing Controls (in the DestinationRouter[] table).

The Tekelec ngHLR performs the Relay processing to a Destination Router in the following scenario:

- The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
- The MSISDN received in the SRI/SRI-LCS message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and received in the SRI/SRI-LCS message)

- The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)
- The subscriber is not TAS registered
- The routing template is set as follows:
  - The routing trigger is set to any other value than 'Never' and is successfully met.
  - The routing type is set to 'Relay'.

The SRI/SRI-LCS Relay call flows are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS request from the G-MSC/G-MLC.
- The Tekelec ngHLR relays the request to the Destination Router based on the information configured in the subscriber's routing template DestinationRouter table.
- The Destination Router replies to the G-MSC/G-MLC with a MAP_SRI_ACK/MAP_SRI_FOR_LCS_ACK.

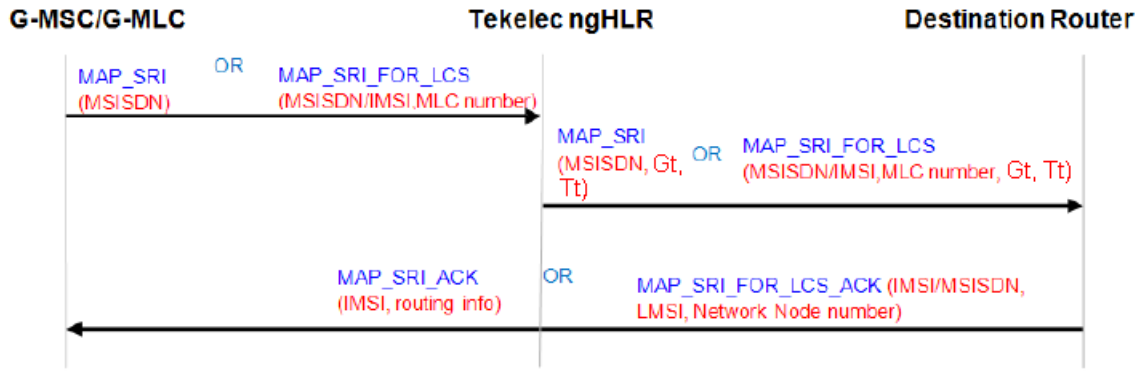


Figure 48: Call flow for SRI/SRI-LCS Relay to a Destination Router within the GSM Network

SRI/SRI-LCS Relay processing to external TAS

The Tekelec ngHLR can relay SRI/SRI-LCS messages to one of the TAS Gt defined in the system's SipTasGt[] table.

The Tekelec ngHLR performs the Relay processing to an external TAS in the following scenarios:

- Scenario 1:
  - The MSISDN received in the SRI/SRI-LCS message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and included in the SRI/SRI-LCS message)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Relay'
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered
- Scenario 2
  - The MSISDN received in the SRI/SRI-LCS message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and included in the SRI/SRI-LCS message)
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)

- The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
- The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered
- The routing template is configured as follows:
  - The routing type is set to 'Relay'
  - The routing trigger is set to one of the following values and is successfully met with the subscriber being TAS registered:
    - 'When SIP Registered'
    - 'When SIP Registered or in HPLMN'
    - 'When SIP Registered or out of HPLMN'

The SRI/SRI-LCS Relay call flows are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS request from the G-MSC/G-MLC
- The Tekelec ngHLR relays the SRI/SRI-LCS request to the external TAS based on the information configured in the SipTasGt table for the TasId stored in the subscriber's registration binding
- The external TAS replies to the G-MSC/G-MLC with a MAP_SRI_ACK/MAP_SRI_FOR_LCS_ACK

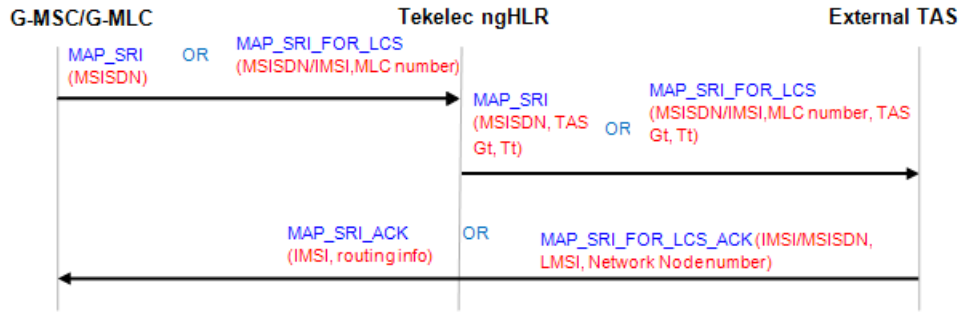


Figure 49: Call flow for SRI/SRI-LCS Relay to the external TAS within the IMS Network

SRI/SRI-LCS Redirect

The Network Operator can configure the Tekelec ngHLR to redirect SRI/SRI-LCS messages to the Home Network's Router, by returning the IMSI and GT address of the Destination Router.

The message can be redirected to:

- G-MSC/G-MLC (in the GSM network)
- External TAS (in the IMS network)

SRI/SRI-LCS Redirect flow to the G-MSC/G-MLC in the GSM Network

The Tekelec ngHLR performs the SRI/SRI-LCS Redirect processing to the G-MSC/G-MLC in the following scenario:

- The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
- The MSISDN received in the SRI/SRI-LCS message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and included in the SRI/SRI-LCS message)
- The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)

- The subscriber is not TAS registered
- The routing template is set as follows:
  - The routing trigger is set to any other value than 'Never' and is successfully met
  - The routing type is set to 'Redirect'

The SRI/SRI-LCS Redirect flows to the G-MSC/G-MLC in the GSM Network are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS message from the originator G-MSC/G-MLC
- The Tekelec ngHLR redirects the SRI/SRI-LCS message by replying to the G-MSC/G-MLC with an IMSI and a Destination Router Gt address based on the Destination Router Gt address configured in the subscriber's routing template DestinationRouter table.

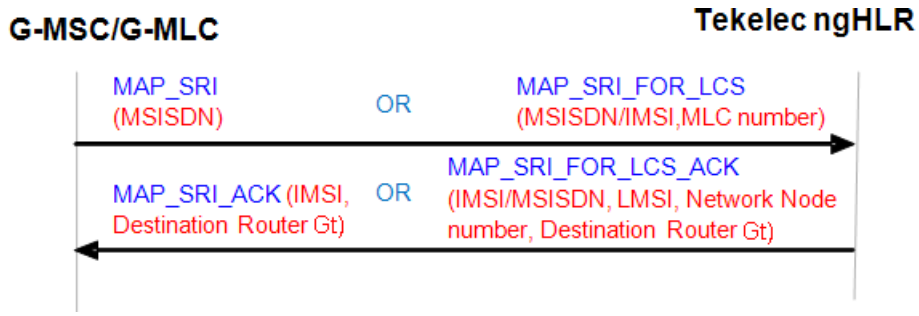


Figure 50: Call flow for SRI/SRI-LCS Redirect to the MSC/VLR (in the GSM network)

SRI/SRI-LCS Redirect to the external TAS in the IMS Network

The Tekelec ngHLR performs the SRI/SRI-LCS Redirect processing to an external TAS in the following scenarios:

- Scenario 1:
  - The MSISDN received in the SRI/SRI-LCS message is known by the Tekelec ngHLR (MSISDN stored in the Tekelec ngHLR's database).
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality's activation status is set to 'Redirect'
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered.

- Scenario 2:
  - The MSISDN received in the SRI/SRI-LCS message is known by the Tekelec ngHLR (it is provisioned in the Tekelec ngHLR and included in the SRI/SRI-LCS message)
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table).
  - The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered.
  - The routing template is configured as follows:
    - Routing type set to 'Redirect'

- The routing trigger must be set to one of the following values and must be successfully met with the subscriber being TAS registered:
  - 'When SIP Registered'
  - 'When SIP Registered or in HPLMN'
  - 'When SIP Registered or out of HPLMN'

The SRI/SRI-LCS Redirect flows to the external TAS in the IMS Network are as follows:

- The Tekelec ngHLR receives a SRI/SRI-LCS message from the G-MSC/G-MLC.
- The Tekelec ngHLR redirects the SRI/SRI-LCS message as follows:
  - The SRI message is redirected by replying to the G-MSC with a MSRN (Redirect Prefix+MSISDN) and an IMSI. The Redirect Prefix sent back in the MAP SRI Ack message indicates to the G-MSC that the call must be routed to the IMS domain.
  - The SRI-LCS message is redirected by replying to the G-MLC with the IMSI and Network Node Number. The Network Node Number sent back in the MAP SRI-LCS Ack message indicates to the G-MLC that the call must be routed in the IMS domain.

  The Tekelec ngHLR retrieves the information returned in the MAP SRI/SRI-LCS message from the SipTasGt table's configuration (Gt address, Tt, Override Tt, Prefix)for the TasId stored in the subscriber's registration binding.
- In the case of the SRI-LCS message, the G-MLC then sends a MAP-PSL (MAP Provide Subscriber Location) message to the external TAS
- In the case of the SRI message, the G-MSC then sends a SIP INVITE message to the CSCF.

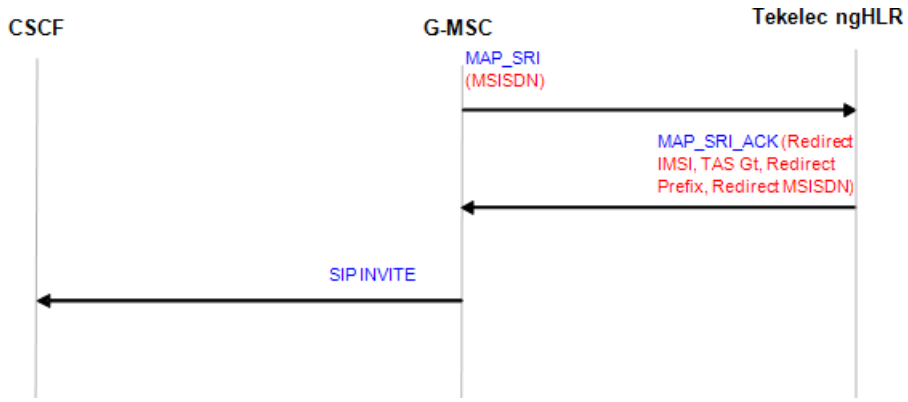


Figure 51: Call flow for SRI Redirect with external TAS (IMS Network)

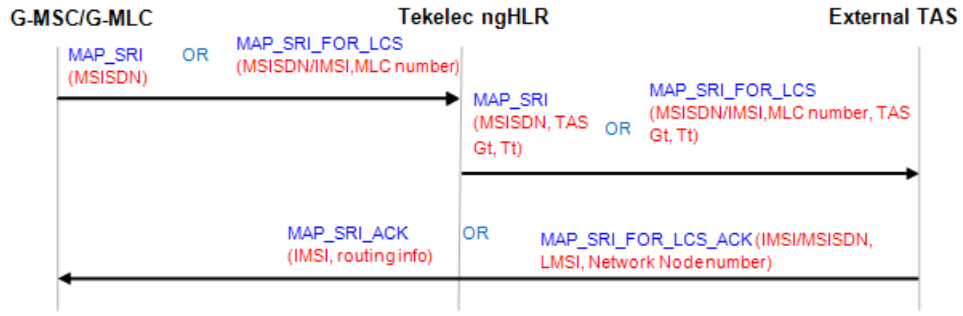


Figure 52: Call flow for SRI-LCS Redirect with external TAS (IMS Network)

ATI Routing

The Tekelec ngHLR can follow the standard MAP ATI processing behavior by responding to a MAP ATI message from the gsmSCF with a MAP ATI Ack message with the subscriber state and location info [IMSI and current MSC address where the subscriber is roaming (currently registered)].

The Tekelec ngHLR can also be configured to relay MAP ATI messages as follows:

- ATI Relay behavior: the Tekelec ngHLR relays the MAP ATI messages from the gsmSCF to one of the following configurable Router:
  - Destination Router (in the GSM network), as per configured in the DestinationRouter table.
  - External HLR (in the GSM network), with the same CdPA and a Tt as per configured in the DestinationRouter table.
  - External TAS (in the IMS network), as per the SIP Registration Bindings and the SipTasGt table.

  The Router then responds to the MAP ATI message by sending to the gsmSCF a MAP ATI Ack message with the location info and subscriber state.

The SDM's provisioning interfaces allow the Network Operator to:

- Activate/Deactivate the ATI Routing functionality, by setting the SriRouting attribute to '1' in the HLR configuration data.
- Define a list of Destination Router addresses (used if mobile device is HLR or SIP registered) and/or a list of SIP TAS Gt (used if mobile device is TAS registered).
- Define various Routing Templates, which will tell the Tekelec ngHLR how to process the MAP ATI message.
  - Define Routing Type (Relay)
  - Define Routing Trigger
  - Define Default Action
  - Associate one of the Destination Router addresses
- Associate a Routing Template to MSISDNs. This allows the Network Operator to control the ATI Routing process on a per subscriber basis.

Note: The Tekelec ngHLR doesn't support the Redirect routing method for MAP ATI messages. If the Routing Template is set to 'Redirect', the Tekelec ngHLR will by default relay the message to the external HLR with the same CdPA as received in the MAP ATI message and as per the configuration in the SipTasGt table for the TasId=0 entry (with the Tt of the TasId 0).

The sections below describe the ATI Routing Template process and each ATI Routing behaviour in details.

ATI Routing Template Process

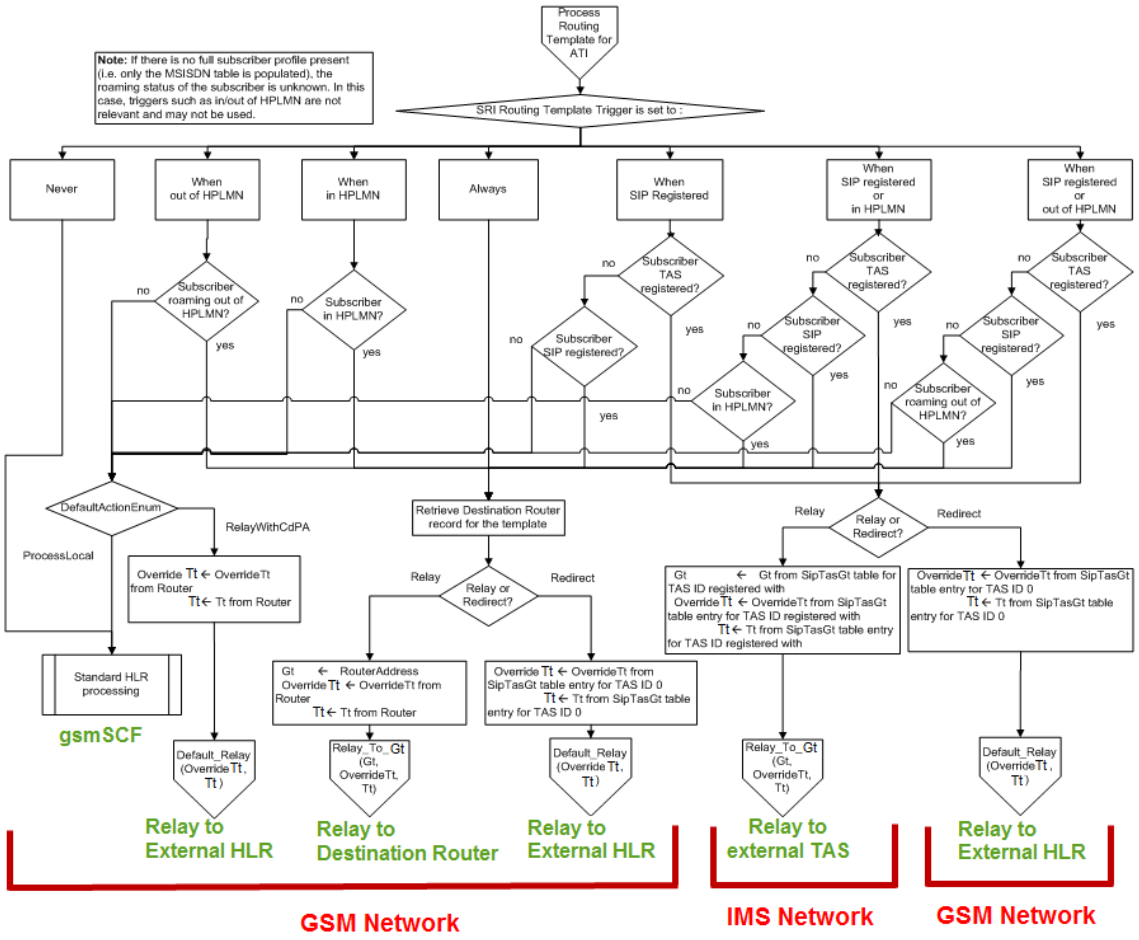


Figure 53: ATI message routing in the Tekelec ngHLR

Table 26: Process Routing Template for ATI Relay

SRI Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
Never		Default Action - Process locally	Process locally-standard HLR process	Responds to ATI with ATI-Ack (IMSI current MSC)	gsmSCF	GSM
When out of HPLMN	Subscriber roaming out of HPLMN	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router (as configured	GSM

SRI Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
					in RouterAddress	
	Subscriber roaming in HPLMN	Default Action - Relay with CdPA	Relay process	Relay ATI (OverrideTt,Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard HLR process	Responds to ATI with ATI-Ack (IMSI current MSC)	gsmSCF	
When in HPLMN	Subscriber roaming in HPLMN	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	GSM
	Subscriber roaming out of HPLMN	Default Action - Relay with CdPA	Relay	Relay ATI (OverrideTt,Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard HLR process	Responds to ATI with ATI-Ack (IMSI current MSC)	gsmSCF	
Always		Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	GSM
When SIP Registered	Subscriber TAS registered	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	External TAS	IMS
	Subscriber SIP registered		Relay	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	GSM
	Subscriber not TAS registered Subscriber not SIP registered	Default Action - Relay with CdPA	Relay	Relay ATI (OverrideTt,Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard HLR process	Responds to ATI with ATI-Ack (IMSI current MSC)	gsmSCF	

SRI Routing Template Trigger is set to:	Subscriber Info	Routing Template Type/Default Action	Process	Action	Destination node	Network Type
When SIP Registered or in HPLMN	Subscriber TAS registered	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	GSM
	Subscriber roaming in HPLMN	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	
	Subscriber roaming out of HPLMN	Default Action - Relay with CdPA	Relay	Relay ATI (OverrideTt,Tt)	External HLR	
		Default Action - Process locally	Process locally-standard HLR process	Responds to ATI with ATI-Ack (IMSI current MSC)	gsmSCF	
When SIP Registered or out of HPLMN	Subscriber TAS registered	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	External TAS	IMS
	Subscriber SIP registered	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	GSM
	Subscriber roaming out of HPLMN	Relay	Relay process	Relay ATI (Gt,OverrideTt,Tt)	Destination Router	
	Subscriber roaming in HPLMN	Default Action - Relay with CdPA	Relay	Relay ATI (OverrideTt,Tt)	External HLR	GSM
		Default Action - Process locally	Process locally-standard HLR process	Responds to ATI with ATI-Ack (IMSI current MSC)	gsmSCF	

Note: If no full subscriber profile present (only the MSISDN table is populated), the roaming status of the subscriber is unknown. In this case, triggers such as in/out of HPLMN are not relevant and are not used.

Standard ATI Processing

The Tekelec ngHLR performs the standard ATI processing in the following scenarios:

- Scenario 1:
  - The SRI Routing functionality is deactivated (HlrConfig's SriRouting attribute set to 0).
- Scenario 2:
  - The subscriber's MSISDN is unknown (not provisioned in the Tekelec ngHLR's database)
  - The SRI Routing functionality's activation status is set to 'Template Only'.
- Scenario 3:
  - The SRI Routing functionality is activated and set to 'Template Only'.
  - The MSISDN received in the ATI message is provisioned in the Tekelec ngHLR.
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN[] table, the SriTemplateId=Null)
- Scenario 4:
  - The SRI Routing functionality is activated (HlrConfig's SriRouting attribute is set to 'Relay', 'Redirect' or 'TemplateOnly').
  - The MSISDN received in the ATI message is provisioned in the Tekelec ngHLR.
  - The MSISDN has a routing template provisioned (SriTemplateId attribute in the MSISDN[] table is set to a supported value that refers to an entry in the RoutingTemplate table).
  - The subscriber's MSISDN has a routing template provisioned with a routing trigger set to 'Never'.
- Scenario 5:
  - The SRI Routing functionality is activated (HlrConfig's SriRouting attribute is set to 'Relay', 'Redirect' or 'TemplateOnly').
  - The MSISDN received in the ATI message is provisioned in the Tekelec ngHLR.
  - The MSISDN has a routing template provisioned (SriTemplateId attribute in the MSISDN[] table is set to a supported value that refers to an entry in the RoutingTemplate table).
  - The routing template provisioned for the subscriber's MSISDN is set as follows:
    - The routing trigger is set to a value other than "Never" and is not successfully met.
    - The default action is set to 'ProcessLocal'.

The standard ATI call flow is as follows:

- The Tekelec ngHLR receives a MAP ATI message from the gsmSCF. The Tekelec ngHLR looks up the MSISDN in the database, the routing template associated to it, the volatile data and registration bindings for that MSISDN.
- The Tekelec ngHLR sends a Provide Subscriber Information (PSI) message to the MSC/VLR, in order to retrieve subscriber data update and status.
- The MSC/VLR replies to the Tekelec ngHLR with a PSI-Ack message including subscriber data status and location information.
- The Tekelec ngHLR sends back a MAP-Ack to the gsmSCF with the information retrieved from the MSC/VLR through the PSI process (i.e. subscriber state and location information).

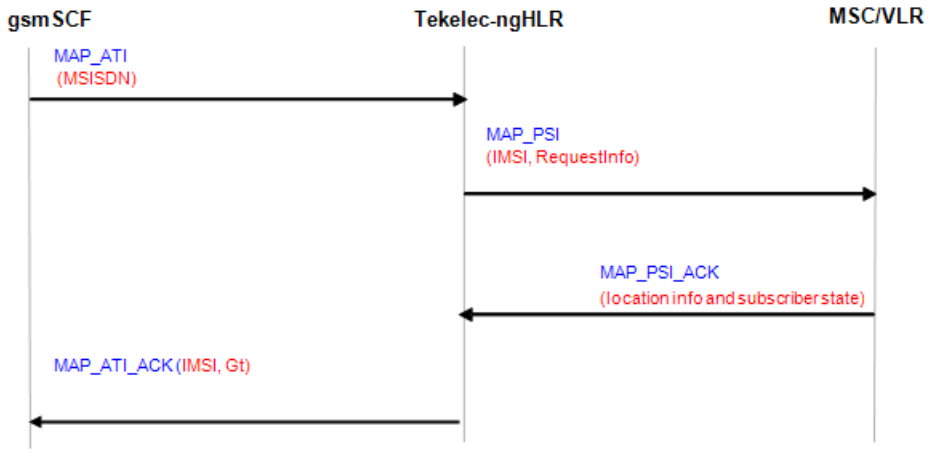


Figure 54: Call flow for Standard ATI Routing

ATI Default Relay to an external HLR in the GSM Network

The Tekelec ngHLR performs the ATI Default Relay with CdPA processing to an external HLR in the following cases:

- Scenario 1:
  - The subscriber's MSISDN is unknown by the Tekelec ngHLR (MSISDN not provisioned in the Tekelec ngHLR).
  - The SRI Routing functionality is activated and is set to 'Relay' or 'Redirect'
- Scenario 2:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (MSISDN provisioned in the Tekelec ngHLR).
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Redirect'
- Scenario 3:
  - The subscriber's MSISDN is known by the Tekelec ngHLR (MSISDN provisioned in the Tekelec ngHLR).
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Relay'
  - The subscriber is not TAS registered
- Scenario 4:
  - The SRI Routing functionality is activated (set to any of the following values: 'Relay', 'Redirect' or 'TemplateOnly').
  - The subscriber's MSISDN is known by the Tekelec ngHLR (MSISDN provisioned in the Tekelec ngHLR).
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)

- The routing template is set as follows:
  - The routing trigger is set to any other value than 'Never' and is not met.
  - The default action is set to RelayWithCdPA.

- Scenario 5:
  - The SRI Routing functionality is activated (set to any of the following values: 'Relay', 'Redirect' or 'TemplateOnly').
  - The subscriber's MSISDN is known by the Tekelec ngHLR (MSISDN provisioned in the Tekelec ngHLR).
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)
  - The routing template is set as follows:
    - The routing trigger is set to any other value than 'Never' and is successfully met.
    - The routing type is set to 'Redirect'.
    - The subscriber is not TAS registered.

- Scenario 6:
  - The SRI Routing functionality is activated (set to any of the following values: 'Relay', 'Redirect' or 'TemplateOnly').
  - The subscriber's MSISDN is known by the Tekelec ngHLR (MSISDN provisioned in the Tekelec ngHLR).
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate entity)
  - The routing template is set as follows:
    - The routing trigger is set to one of the following values and is successfully met with the subscriber being TAS registered:
      - When SIP registered
      - When SIP registered or in HPLMN
      - When SIP registered or out of HPLMN
    - The routing type is set to 'Redirect'.

Note: Since the Tekelec ngHLR doesn't support the redirect capability for MAP ATI messages, if the routing type is set to 'Redirect', the Tekelec ngHLR will always perform a Default Relay to the external HLR, by relaying the message with the same CdPA as received.

The ATI Default Relay call flow to an external HLR in the GSM Network is as follows:

- The Tekelec ngHLR receives a MAP ATI request from the gsmSCF.
- The Tekelec ngHLR relays the request to the external HLR with the same CdPA and possibly a different Tt, as per configured in the DestinationRouter table or in the SipTasGt table. In the scenarios 1,2,3,5 and 6, described above, the Tekelec ngHLR reads the Override Tt and Tt information from the SipTasGt table for the TasId=0 entry. In the scenario 4, the Tekelec ngHLR reads the Override Tt and Tt information from the DestinationRouter table.
- The external HLR replies to the gsmSCF with a MAP_ATI_Ack.

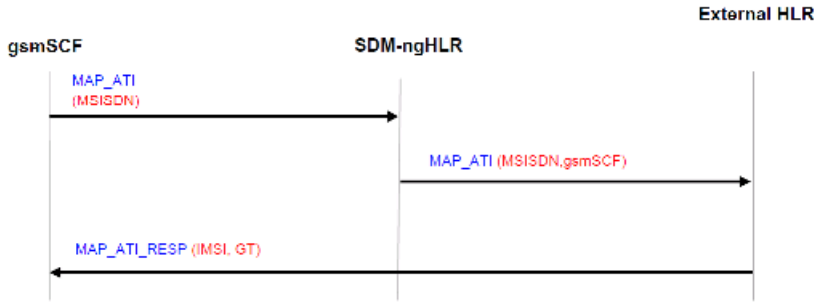


Figure 55: Call flow for ATI Relay to the external HLR within the GSM Network

ATI Relay to a Destination Router in the GSM Network

The Tekelec ngHLR can relay ATI messages to one of the Destination Routers defined in the system's Routing Controls (in the DestinationRouter[] table).

The Tekelec ngHLR performs the ATI Relay process to a Destination Router in the following scenario:

- Scenario 1:
  - The MSISDN received in the ATI message is known by the Tekelec ngHLR (MSISDN provisioned in the Tekelec ngHLR).
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)
  - The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
  - The routing template is configured as follows:
    - The routing type is set to 'Relay'
    - The routing trigger is set to any other value than 'Never' and is successfully met.
    - The subscriber is not TAS registered.

The ATI Relay to Destination Router call flow is as follows:

- The Tekelec ngHLR receives a MAP ATI request from the gsmSCF.
- The Tekelec ngHLR relays the request to the Destination Router as per the configuration in the DestinationRouter table (Gt, Override Tt, Tt).
- The Destination Router replies back to the gsmSCF with a MAP_ATI_Ack.

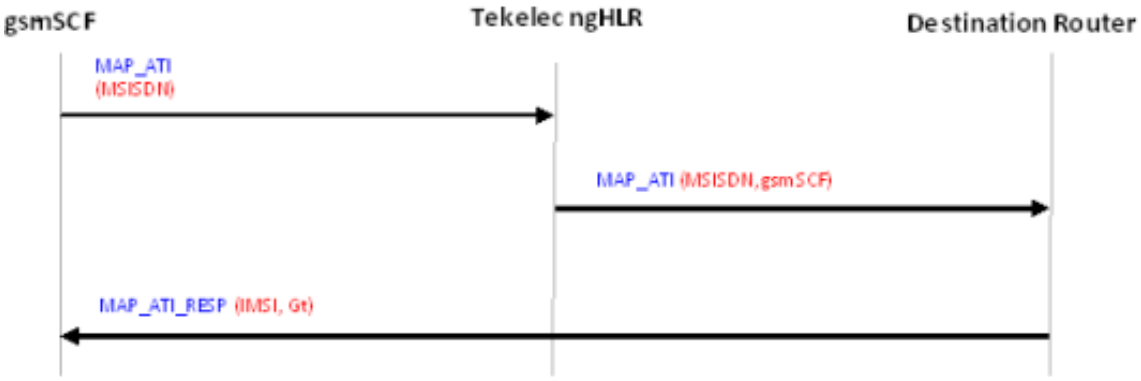


Figure 56: Call flow for ATI Relay to the Destination Router within the IMS Network

ATI Relay flow to the external TAS in the IMS Network

The Tekelec ngHLR can relay ATI messages to one of the TAS GT defined in the system's SipTasGt[] table.

The Tekelec ngHLR performs the ATI Relay processing to an external TAS in the following scenarios:

- Scenario 1:
  - The MSISDN received in the ATI message is known by the Tekelec ngHLR (MSISDN is provisioned in the Tekelec ngHLR)
  - The subscriber doesn't have a routing template provisioned in the database (in the MSISDN table, the SriTemplateId=Null)
  - The SRI Routing functionality is activated and set to 'Relay'
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered
- Scenario 2
  - The MSISDN received in the ATI message is known by the Tekelec ngHLR (MSISDN is provisioned in the Tekelec ngHLR)
  - The subscriber has a routing template provisioned in the database (in the MSISDN table, the SriTemplateId is set to a supported value that refers to an entry in the RoutingTemplate table)
  - The SRI Routing functionality is activated (set to 'Relay', 'Redirect' or 'TemplateOnly')
  - The subscriber has a SIP profile provisioned in the Tekelec ngHLR (AddressOfRecord and Registration Bindings) and is TAS registered
  - The routing template is configured as follows:
    - Routing type set to 'Relay'
    - The routing trigger is set to one of the following values and is successfully met with the subscriber being TAS registered:
      - 'When SIP Registered'
      - 'When SIP Registered or in HPLMN'
      - 'When SIP Registered or out of HPLMN'

The ATI Relay call flow to the external TAS in the IMS Network is as follows:

- The Tekelec ngHLR receives a MAP ATI request from the gsmSCF.
- The Tekelec ngHLR relays the request to the TAS, by changing the CdPA and possibly the Tt with the TAS Gt and Tt configured in the SipTasGt table for the TasId entry defined by the SIP Registration Bindings.
- The TAS replies to the gsmSCF with a MAP_ATI_Ack.

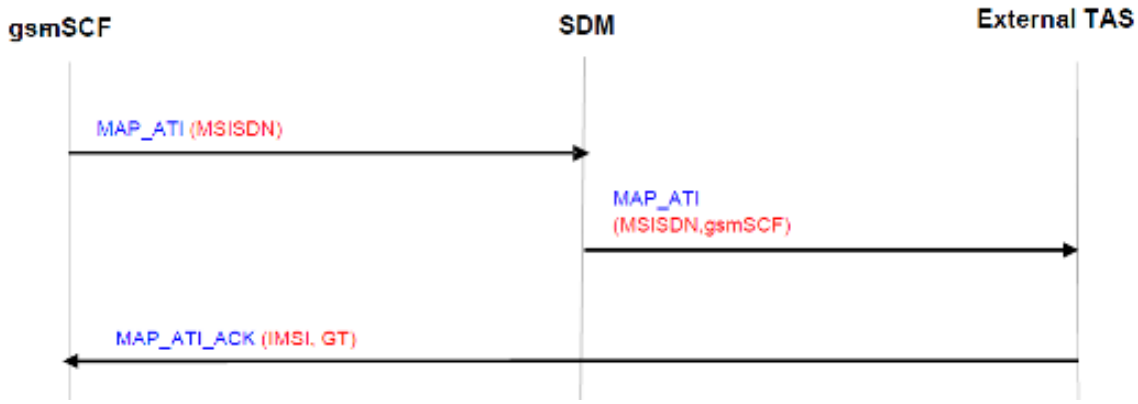


Figure 57: Call flow for ATI Relay to the external TAS within the IMS Network

Support of MNP-SRF (Mobile Number Portability)

With the implementation of this feature, the Tekelec ngHLR now supports Mobile Number Portability (MNP), which allows mobile subscribers to change their subscription from one service provider to another without changing their mobile phone number (MSISDN). A subscriber that has kept the same phone number after changing from one service provider to another is said to have a “ported” phone number (MSISDN). Hereunder are other terms used for the MNP:

- Number range holder network: network from which the "ported" number is coming from.
- Recipient network (or subscription network): network to which the "ported" number is migrating to.
- Originating network: network originating a query call (call, SMS, non-call related SS7 message) for an MSISDN that has been ported.
- Visited network: network on which the subscriber with a "ported" number is roaming to.

The Mobile Number Portability has been implemented by including the following Signaling Relay-based solution in the HLR service. The MNP-SRF logical function is composed of two key parts:

- The Number Portability Location Register (NPLR), a MAP entity containing the MNP logic
- The Number Portability Database (NPDB), a storage of information related to the porting status of MSISDNs.

The Tekelec ngHLR supports both the NPLR and NPDB. The Tekelec NPDB is managed independently from the Tekelec ngHLR subscriber profiles and contains, for each MSISDN provisioned as “ported out”, the following:

- MSISDN (key),
- Porting status (ported in, not ported out, ported out),
- Routing Number (e. 164 format),

- Routing Method (Relay or Redirection)

The Network Operator has full control over the content of the NPDB by being able to provision the Number Portability data for each “ported” MSISDN and by being able to provision the IMSI that must be returned in the SRI-ack when the Tekelec ngHLR redirects the interrogating node to the recipient's network.

The information contained in this database supersedes the one contained in the "regular" subscriber profile, if any. This means that a subscriber can be marked as "ported out" in the NPDB, even though its record still exists in the Hlr database.

The MNP-SRF functionality can be authorized (made available) only by the Tekelec *Customer Care Center*. By default, it is unavailable and cannot be activated. Once authorized, it remains deactivated by default and the Network Operator can activate/deactivate it dynamically during running time of the system by executing the ActivateFeature() and DeactivateFeature() operations from the CLI or using XML scripts or can also simply activate/deactivate it from the WebCI's HLR Configuration. Please note that the PortedOut database can be modified while the MNP-SRF is deactivated.

Once the MNP-SRF functionality is activated, it is triggered by the following incoming MAP messages for a subscriber with a “ported out” MSISDN:

- Call related messages:
  - Send Routing Info (SRI)
- Non-call relate messages:
  - Set Message Waiting Data (SMWD)[2]
  - Report SM Delivery Status (SMDEL)[3]
  - Send Routing Info for Short Message (SRI-SM)
  - Send IMSI (SNDIMSI)
  - Report SM Delivery Status (ReportSM-DS)
  - Any Time Interrogation (ATI)

Once an MSISDN is ported out, the queries for the ported MSISDN are still directed to the Number range holder network. The MNP-SRF functionality of the Number range holder network's Tekelec ngHLR takes one of the following actions:

- Continue normal HLR processing
- Relay query towards the recipient network
- Redirect interrogating node towards the recipient network

The Tekelec ngHLR's MNP-SRF functionality decides which action to take depending on the information found in the NPDB for the subscriber, as follows:

- If the subscriber's MSISDN is not present in the NPDB, the Tekelec ngHLR continues with the normal HLR logic by completing the MAP transaction, which includes the following
  - Retrieving the IMSI from the Tekelec ngHLR's database
  - Retrieving the full subscriber profile
  - Processing the message
- If the subscriber's MSISDN is not present in the NPDB or in the Tekelec ngHLR's database (not defined in the MSISDN entity), then the query is answered with an error as per normal HLR procedures.

- If the subscriber's MSISDN porting status is “ported in” or “not ported out”, the Tekelec ngHLR continues with the normal HLR logic.
- If the incoming MAP message is non-call related and in the case where the subscriber's MSISDN, for which the message was received, is present in the NPDB and has a porting status set as “ported out”, the Tekelec ngHLR relays the MAP message query towards the recipient network, as follows:[1] [2]
  - When relaying an incoming query, the MNP-SRF doesn't modify the MSISDN contained at the MAP layer, but modifies the SCCP layer as follows:
    - SCCP CdPA = Routing Number (RN) stored in NPDB
    - SCCP CgPA = Interrogating network element GT
- If the incoming MAP message is call related and in the case where the subscriber's MSISDN, for which the message was received, is present in the NPDB (which means that the MSISDN is “ported out”) and the routing method is set as “relay”, the Tekelec ngHLR relays the MAP message query towards the recipient network as follows:
  - When relaying an incoming query, the MNP-SRF shall not modify the MSISDN contained at the MAP layer, but shall modify the SCCP layer as follows:
    - SCCP CdPA = Routing Number (RN) stored in NPDB
    - SCCP CgPA = Interrogating network element GT
- If the incoming MAP message is call related and in the case where the subscriber's MSISDN, for which the message was received, is present in the NPDB (which means that the MSISDN is “ported out”) and the routing method is set as “redirection”, the Tekelec ngHLR redirects the MAP message query towards the recipient network as follows:
  - When redirecting an incoming query, the MNP-SRF replies to the SRI with an SRI_ack as follows:
    - MSRN = Routing Number (RN) stored in the NPDB
    - IMSI = generic IMSI with MCC/MNC of the recipient network
- If the incoming MAP message is a MAP Any Time Interrogation (ATI) and in the case where the subscriber's MSISDN, for which the message is received, is present in the NPDB, the Tekelec ngHLR replies to the ATI with the content of the NPDB for the given MSISDN.

The following table summarizes the expected Tekelec ngHLR action upon reception of MAP messages when the MNP-SRF is active

Table 27: Tekelec ngHLR action upon reception of MAP messages when MNP-SRF active

Incoming Query	MSISDN porting status	MSISDN routing method	Action
SRI	Ported out	Relay	Forward SRI to RN

[1] [2] Equivalent of SMDEL in Map v1
[2] [3] Equivalent of SMWD in Map v2 and v3

		Redirection	Reply with SRI-ack with MSRN=RN
	Ported in	n/a	Reply with normal SRI-ack
	Not ported out	n/a	Reply with normal SRI-ack
	Absent from NPDB	n/a	Reply with normal SRI-ack
SRI-SM, SMWD, ReportSM-DS, SendIMSI, ATI	Ported out	n/a	Forward query to RN
	Ported in	n/a	Reply with normal query response
	Not ported out	n/a	Reply with normal query response
	Absent from NPDB	n/a	Reply with normal query response

The Redirection routing method only applies to SRI messages. All other messages are automatically forwarded to the remote network using the Relay touring method.

To achieve this, the following has been implemented in the Tekelec ngHLR and can be provisioned by the operator from the WebCI and CLI:

- The HlrConfig's MobileNumberPortability attribute has been added to the HlrConfig entity in order to allow the Network Operator to view dynamically the MNP activation state. If the Tekelec *Customer Care Center* has authorized (made available) the MNP functionality, this authorizes the Network Operator to activate or deactivate the feature by executing the ActivateFeature() or DeactivateFeature() operations through the CLI or by clicking on the Activate or Deactivate buttons next to the MobileNumberPortability field in the WebCI's HlrConfig provisioning window.
- The MnpPortedOut entity can be provisioned from the WebCI's Mnp table in the Mobile Number Portability window. This table allows the operator to provision the Number Portability data for each “ported” MSISDN.
- The MnpImsiForRedirect entity allows the operator to provision the IMSI (generic IMSI with MCC/MNC of the recipient network) that must be returned in the SRI-ack when the Tekelec ngHLR redirects the interrogating node to the recipient's network.

In addition to this, the following counters have been implemented to count:

- The number of queries for "ported out" MSISDNs and relayed to the recipient network
- The number of queries received for “ported out” MSISDNs and redirected to the recipient network

For more details on the counters implemented, refer to the *SDM Performance Measurements* document. For more details on the Mnp and ImsiForRedirect entities, refer to the *“MNP-SRF (Mobile Number Portability)”* section of the *SDM Subscriber Provisioning – Reference Manual*.

For more details on the CLI's ActivateFeature() and DeactivateFeature() operations, refer to the *“ HLR Operations”* section in the *SDM System Configuration – Reference Manual*. For instructions on how to view the activation status and activate/deactivate the MNP feature from the WebCI, refer to the *“Viewing activation status of HLR features and activating/deactivating them individually”* section of the *SDM System Configuration – User Guide*.

For instructions on how to provision MNP-SRF subscribers from the WebCI, refer to the "Viewing/Editing MNP-SRF subscribers" section of the SDM Monitoring, Maintaining, Troubleshooting – User Guide.

MNP support for number ranges

The MNP Support for Number Ranges feature is an enhancement to the MNP-SRF feature.

Description

The MNP Support for Number Ranges feature allows the operator to pre-provision a range of MSISDNs belonging to other licensed operators (OLOs) as well as foreign numbers for which the porting status is still unknown.

A request targeted to a number of a foreign network that is not ported-in will be rejected by the Tekelec ngHLR because the number is provisioned neither in the MNP database nor in the Tekelec ngHLR database. The Tekelec ngHLR will reject the request with the error "unknown subscriber". The request must then be handled by an external system, such as SMSC or GMSC.

In addition to the ported MSISDNs, the operator provisions a number range in a new table dedicated to non-ported OLO subscribers. The table provides an association between the number range and a routing number belonging to the number-range owner network. The operator can also provision foreign numbers that have been ported out to a foreign network in the number portability database (NPDB).

Configuration

This feature can be configured through the Tekelec CLi, WebCI, or XML interface. These tables are affected by this feature:

- HlrMnpMsisdnRange - New

The HlrMnpMsisdnRange table allows the Network Operator to define MSISDN Ranges for OLO numbers that are not known to be ported. These numbers are not part of the "Own Number Range" of the Tekelec ngHLR

- Msisdn - Modified
  - Porting Status: The set of values have been redefined
- HlrMnpPortedOut- Modified
  - Ruleld-Added
  - ActiveSubsTimestamp-Added
  - RoutingNumber-Moved to table HlrMnpRoutingRule
  - RoutingMethodForSri-Moved to table HlrMnpRoutingRule
  - Imsild-Deleted

Alarms

No new alarms have been implemented in this feature.

MNP DB mismatch error handling

The MNP DB Mismatch Error Handling feature is an enhancement to the MNP-SRF feature

Description

The MNP DB Mismatch Error Handling feature allows the Tekelec ngHLR Mobile Number Portability (MNP) feature to recognize second queries to the Number Portability database (NPDB) based on database configuration mismatches between the home network and the networks of other-licensed operators (OLOs). This feature eliminates the network inefficiencies and potential signaling loops caused by the current error handling method.

The second query on an incoming call-related or non call-related message is currently determined by the detection of the Own Network prefix (routing number) in the Called Party Address (CdPA) of the SCCP header. A string comparison algorithm in the CdPA layer determines the mismatch. The CdPA can contain these combinations of Tekelec ngHLR routing number (RN), country code (CC) and Subscriber MSISDN:

- RN only (0)
- CC + RN + MSN (1)
- RN + CC + MSN (2)
- RN + MSN only (3)
- MSN only (4)

The MNP DB Mismatch Error Handling feature recognizes these types of mismatches:

- Type A : Foreign network has the subscriber ported to the home network, but the subscriber is ported out in the home Number Portability database (NPDB). The home NPDB is the number range holder.
- Type B : Foreign network has the subscriber ported to the home network, but the subscriber is not in the Tekelec ngHLR (or NPDB).
- Type C : Foreign network has the subscriber ported to the home network, but the subscriber is ported out in the home NPDB. The home NPDB is not the number range holder.

Configuration

This feature can be configured through the Tekelec CLi, WebCI, or XML interface. These tables have been added or modified:

- HlrMnpHplmnRouting - New

This table holds the RN for the home network and is used to detect incoming database mismatch cases.

- MnpHplmnMsisdnRange - New

This table allows the Network Operator to define the MSISDN Own Number Range of the Tekelec ngHLR and it is used to detect the different loop conditions (A and C).

- MnpRoutingRule - New

This table allows the Network Operator to define rules used to build routing numbers for outgoing messages.

Alarms

These new alarms are generated for the respective mismatch type.

Alarm ID	Name	Description	Severity
9252	MnpDbMismatchTypeA	MNP DB-Mismatch Type A	Warning
9253	MnpDbMismatchTypeB	MNP DB-Mismatch Type B	Warning

Alarm ID	Name	Description	Severity
9254	MnpDbMismatchTypeC		

Counters:

These new counters apply to the MNP DB Mismatch Error Handling features:

- Number of SRI queries received for Number Range MSISDNs and redirected to the recipient network.
- Number of SRI queries received for Number Range MSISDNs and relayed to the recipient network.
- Number of SRI-SM queries received for Number Range MSISDNs and relayed to the recipient network.
- Number of Send-MWD queries received for Number Range MSISDNs and relayed to the recipient network.
- Number of SM-DEL queries received for Number Range MSISDNs and relayed to the recipient network.
- Number of Send-IMSI queries received for Number Range MSISDNs and relayed to the recipient network.
- Number of ATI queries received for Number Range MSISDNs and relayed to the recipient network.
- Number of queries resulting in a DB-Mismatch Type A.
- Number of queries resulting in a DB-Mismatch Type B.
- Number of queries resulting in a DB-Mismatch Type C.
- Number of ATI queries received for any MSISDNs and containing the field MnpInfoRequest.

SIP-AS

Fixed-Mobile Convergence functionality

The Fixed-Mobile Convergence (FMC) functionality provides the Tekelec ngHLR with the capability of integrating subscriber profiles from the GSM network domain (HLR) and the SIP network domain (SIP Registrar) so that they can be managed together.

An integrated subscriber profile significantly reduces network complexity and operational expenditures, allowing subscriber's profiles to be provisioned in a single system, and enabling new and enhanced call-termination routing opportunities.

Specifically, the FMC feature supports the following functionalities:

- SIP Registrar Function, including authentication and authorization
- Domain Selection Function
- SIP Redirect Function with SIP-anchored domain selection
- GSM registration agent (SIP User Agent)

The Tekelec ngHLR allows the operator to selectively enable/disable individually the following SIP functional components:

- SIP Registrar
- SIP Redirect Server
- GSM Registration Agent

This way, the Tekelec ngHLR can achieve the appropriate functional behavior according to the operator's network.

The Tekelec ngHLR can support four deployment models:

1. Model1: GSM-anchored FMC (SIP Server = SIP Registrar + Domain Selection Function)
2. Model2: SIP-anchored FMC (SIP Server = GSM Registration Agent + SIP Redirect Server)
3. Model3: SIP-anchored FMC (SIP Server = SIP Registrar + Domain Selection Function + SIP Redirect Server)
4. Model4: SIP-anchored FMC for GSM-only subscribers (SIP Server = SIP Redirect Server + Domain Selection Function)

In both models 1 and 3, the SIP Server of the Tekelec ngHLR has the role of a SIP Registrar. The Tekelec ngHLR's FMC Server with the SIP Registrar functionality accepts SIP Register requests enabling SIP UAs to register and deregister their location. SIP subscribers must first have their SIP AORs provisioned as SIP subscriber profiles in the Tekelec ngHLR's database before they can register. The SIP Registrar functionality enables the Tekelec ngHLR to store these locations in its database which also allows it to provide location services.

The Tekelec ngHLR can also play the role of a SIP Redirect Server, if this functionality is enabled, by accepting a SIP Request from a UA for the called party destination address. In response to the request, it finds out the address where the called party has logged on, by interacting with the Tekelec ngHLR's (SIP Registrar functionality) database which contains the information on the location of the registered SIP UAs, and sends back the required address to the UA.

In model 3, the SIP Server of the Tekelec ngHLR plays the role of a SIP Redirect Server, in addition to the one of a SIP Registrar and DSF, by returning the contact information using a SIP Redirect response.

In model 2, the primary network registrar is located in the SIP domain (this can be either the IMS network or the pre-IMS SIP network). In that case, the SIP Registrar is external and the Tekelec ngHLR acts as a gateway between the GSM mobile network and the SIP network. The GSM registration agent registers GSM subscribers with an external SIP Registrar, thus making GSM devices appear as SIP end-points. The GSM registration agent uses the provisioned SIP subscriber information to send a SIP register to an external registrar. The Tekelec ngHLR then receives SIP Invite requests for GSM subscribers and acts on these requests by obtaining a routing number (MSRN) for the GSM subscriber from the VLR. Finally, the Tekelec ngHLR also plays the role of a SIP Redirect Server in model 2, by returning the routing number to the SIP domain using a SIP Redirect response.

Model 4 is a subset of the generic Model 3, but where no SIP Registrar functionality is needed. The Tekelec ngHLR maintains only GSM MAP registration information and provides a subscriber's GSM location in response to a SIP Invite request.

The Tekelec ngHLR supports the http-Digest (Digest MD5) authentication for incoming and outgoing registrations. SIP registration and deregistration is triggered by GSM attach and detach events which are processed by the Tekelec ngHLR through its HLR module and which then causes a SIP register or deregister request to be generated.

If a SIP registration with the external SIP Registrar (Typically, in an IMS network the external SIP Registrar's functionalities are covered by the CSCF) is refused or fails, the Tekelec ngHLR will perform a deregistration on the GSM network in order to keep the subscribers registration state consistent. The GSM registration agent maintains the registration state of all active subscribers, including expiry times. Prior to expiry, the GSM registration agent performs a re-register in order to keep the SIP registration active.

By performing a SIP Register with the SIP Registrar, it will now direct incoming Invite requests to the registered address. Unlike a SIP UA which can process SIP Invite requests, the GSM registration agent

relies on the Tekelec ngHLR SIP Redirect Server to process incoming Invite requests. To achieve this, the registration contact info provided is the SIP Redirect Server contact info.

SIP Registrar

The SIP Registrar functional element is integrated within the Tekelec ngHLR. Compatible with IETF (Internet Engineering Task Force) standards, the SIP Registrar plays a similar role in SIP based, Voice-over-IP (VoIP) networks as the 3GPP HLR/AuC plays in GSM networks. Subscribers with a VoIP subscription, either via a SIP phone, terminal adapter, dual-mode handset or simple SIP software client, can access voice services by registering and authenticating with a Registrar. Soft-switches and Proxies can then query the Registrar to obtain the Contact URI (Uniform Resource Identifier) associated with the public Address-of-Record (AoR).

Domain Selection Function

The Domain Selection Function element is also integrated within the Tekelec ngHLR. Its role is to provide an intelligent, routing decision point for incoming voice calls destined to a multi-mode subscriber, thus seamlessly solving one inherent problem of Fixed Mobile Convergence: the Network Domain Selection. When the HLR receives a MAP message requesting for a subscriber's location, the DSF determines the optimal routing destination based on the registration status of the subscriber (GSM-only, SIP-only, GSM and SIP), the subscriber preferences, and the operator's preferences. The DSF provides the same services for calls coming from the VoIP domain into the SIP Redirect Server. In future releases, the DSF will evolve to comply with the 3GPP IMS Voice Call Continuity (VCC) framework.

SIP Redirect function with SIP-anchored domain selection

The SIP Redirect function is as per RFC 3261, except where noted. This functional component provides traditional SIP Redirect Server functionality augmented with domain selection. Once the Registrar performs SIP Register/Deregister tasks, the Tekelec ngHLR then receives SIP Invite requests from the SIP domain. Then the Tekelec ngHLR then performs the domain selection function and selects the best contact for the subscriber based on registration information from both the GSM and SIP domains. Selecting a GSM contact results in the Tekelec ngHLR retrieving a GSM roaming number from the VLR. The Tekelec ngHLR then returns the contact information using a SIP Redirect response. The returned contact selected is based on the operator configuration of the Tekelec ngHLR behavior, the subscriber preferences and the registered contacts. The Tekelec ngHLR supports the SIP contact type to registration bindings concept. The contact type allows the Tekelec ngHLR to perform call mediation when responding to SIP Invite requests. These contact types are: GSM, SIP and temporary contacts provisioned by the operator.

The redirect server supports the following features:

- It responds to SIP INVITE requests, CANCEL requests and ACK requests.
- It performs authorization of Invite requests.
- It maintains transaction state for an entire SIP transaction.

As for the SIP Redirect function, it supports the configurable domain name in the contact header in the 302 Redirect answer and the expiration associated to it.

Subscriber Information in a 30x (302/303) Response

The Tekelec ngHLR SIP Redirection Server can receive a SIP INVITE message for a provisioned Address of Record, and in some conditions, can return a 300/302 response to indicate how to route the session.

The 300/302 response includes a number of contact URIs that can also include the GSM Mobile Station Routing Number (MSRN) or GSM Forward-to Number (FTN).

With the "Subscriber Information in a 30x Response" feature, the operator can configure the Tekelec ngHLR Sip RedirectServer to include additional information in a 30x Response. This can help call processing by being able to retrieve from the Tekelec ngHLR more information on the subscriber, such as the following:

- Subscriber's active IMSI
- Subscriber's currently-registered VLR or SGSN address

With this feature, the operator can provision the following parameters through the CLI:

- The "IsAdditionalInfoEnabled" parameter can be provisioned in the RedirectServer entity. Provisioning this parameter indicates to the Tekelec ngHLR SIP Redirect Server whether or not a "Message Body" needs to be included in the 30x Response message. If this parameter is provisioned to include a "Message Body" in the 30x Response message, the following additional information will be inserted in the "Message Body":
  - Timestamp : Field that provides the local system time when the SIP 30x message was generated.
  - ActiveImsi: Field that indicates current active IMSI for subscribers with Multi-IMSI feature activated.
    - For subscribers without Multi-IMSI the value of ActiveImsi is the same as primary IMSI.

- The "IsGsmLocationInfoIncluded" parameter can also be provisioned in the RedirectServer entity. Provisioning this parameter indicates to the ngHLR SIP Redirect Server whether or not to send, in addition to the Timestamp and ActiveImsi, the following subscriber information in the 30x Response 's "Message Body" :
  - VlrNumber : Field that indicates the VLR number from which last MAP-UpdLoc was received by Tekelec ngHLR for subscribers that are GSM attached.
    - For subscribers that are not GSM attached, are not reachable, or have no GSM profile, the VlrNumber is zero.
  - SgsnNumber: Field that indicates the SGSN Number to which subscriber is attached for subscribers that are GPRS attached.
    - For subscribers that are not GPRS attached, are not reachable, or have no GSM profile, the SgsnNumber is zero.

Through the WebCI, the configuration of these parameters can only be viewed.

The additional information appears in XML format in the "Message Body" section of either the 302 Moved Temporarily or 300 Multiple Contacts messages.

When the "Message Body" is included in a SIP INVITE message, the Tekelec ngHLR's SIP Redirect Server sends a header indicating that the handling of the "Message Body" is "optional" in order to allow the 30x Response message to be able to traverse any 3rdparty SIP proxies located between the operator's proxy and Tekelec ngHLR.

Hereunder is an example of a 30x Response sent by the Tekelec ngHLR if the subscriber is registered as a GSM contact and if the SIP Redirect Server configuration is set as follows:

- "IsAdditionalInfoEnabled" parameter is set to "On"

- "IsGsmLocationInfoIncluded" parameter is set to "On"

```
SIP/2.0 302 Moved Temporarily
From: <from details>
To: <to details>
Contact: <returned GSM contact>
Content-Disposition: render; handling="optional"
Content-Type: application/xml; charset="utf-8"
Content-Length: <length of message body in octets>
<?xml version='1.0' encoding='UTF-8'?>
<AdditionalInfo>
   <Timestamp>2008-01-28 19:55:23</Timestamp>
   <SubscriberInfo>
      <ActiveImsi>112233445566778</ActiveImsi>
      <VlrNumber>15149329701</VlrNumber>
      <SgsnNumber>15149329701</SgsnNumber>
   </SubscriberInfo>
</AdditionalInfo>
```

Note: In the case where the subscriber is only SIP registered, the Tekelec ngHLR sends a 30x Response that does not include the Timestamp and GSM SubscriberInfo, even if the IsAdditionalInfoEnabled and IsGsmLocationInfoIncluded flags are ON.

For more information on the AccessRestrictedData and the parameters to provision, refer to the "*Access Restriction Data"* section of the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision this entity, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Hereunder is an example of a 30x Response sent by the Tekelec ngHLR if the GSM subscriber is not registered, but has CFU and/or CFNRc activated and if the SIP Redirect Server configuration is set as follows:

- "IsAdditionalInfoEnabled" parameter is set to "On"
- "IsGsmLocationInfoIncluded" parameter is set to "On

```
SIP/2.0 302 Moved Temporarily
From: <from details>
To: <to details>
Contact: <returned GSM contact>
Content-Disposition: render; handling="optional"
Content-Type: application/xml; charset="utf-8"
Content-Length: <length of message body in octets>
<?xml version='1.0' encoding='UTF-8'?>
<AdditionalInfo>
   <Timestamp>2008-01-28 19:55:23</Timestamp>
   <SubscriberInfo>
      <ActiveImsi> </ActiveImsi>
      <VlrNumber> </VlrNumber>
      <SgsnNumber> </SgsnNumber>
   </SubscriberInfo>
</AdditionalInfo>
```

Note: In the case where the subscriber is only SIP registered, the Tekelec ngHLR sends a 30x Response that does not include the Timestamp and GSM SubscriberInfo, even if the IsAdditionalInfoEnabled and IsGsmLocationInfoIncluded flags are ON.

For more information on the AccessRestrictedData and the parameters to provision, refer to the "*Access Restriction Data"* section of the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision this entity, refer to the "Viewing/Editing a HLR Service Profile" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

30x (302/303) response for call forwarding cases

With the implementation of this feature, the Tekelec ngHLR now returns a specific code in the `SIP INVITE 30x` response for a subscriber in one of the following call forwarding cases:

- `Call Forward Unconditional` (cause code: 302)
- `Call Forward Not Reachable`(cause code: 503)

For these two cases, the URI parameter 'cause' along with the associated code is added to the `SIP INVITE 30x` response, within the Contact header that contains GSM/HLR information.

The addition of the 'cause' parameter doesn't cause any interoperability issues since, as per the RFC 3261, SIP proxies that don't understand this uri-parameter must simply ignore it.

Handling of SS7 and SIP abnormal failure cases

This feature has been implemented to add intelligence to the Tekelec ngHLR when handling SS7 and SIP abnormal failure cases. New SIP error codes have been implemented and the Tekelec ngHLR now returns SIP INVITE responses with more meaningful error codes. As a result, this allows the SIP Client Application to react more accurately.

The Tekelec ngHLR can now include the following SIP error codes in the SIP INVITE response:

- `Temporary Unavailable (error code: 480)`. This error code is returned in one of the following cases:
  - the subscriber is provisioned but no MSRN or Call Forward Number can be allocated to it in the case of a normal failure (i.e. Mobile phone is turned OFF or not reachable). If in this case SIP registration bindings are found, a 30x message with no 'GSM Contact' is returned.
  - No answer is received from the VLR in SS7 and SIP abnormal failure cases, such as:
- All SS7 links are down
- An error is received from the VLR (other than mobile not reachable (no MSRN))
  - `Not Found (error code:404)`. This error code is returned in the case where:
    - The subscriber is not found/provisioned in the database.
  - `Internal Server Error (error code:500).` This error code is returned in the case where:
    - SIP internal processing/resource issues.
    - HLR/SIP processes cannot communicate.
    - HLR internal processing/resource issues.
- Upon reception of 500 errors, the SIP UA client application should be switched to the geo-redundant node (if applicable).

In addition, new operations have been implemented in the SIP Server in order to allow the SIP Client Application to react more accurately in the case where it communicates with two SDM systems working in a geo-redundant mode.

In the cases where the SIP Client Application should route all the SIP transactions from the troubled site to the healthy site, the following operations have been implemented in the Tekelec ngHLR:

SIP Redirection Server CAMEL interaction

With the implementation of this feature, the Tekelec ngHLR can now return Camel information (T-CSI information) in the `SIP INVITE` response for a subscriber with both a SIP and GSM profile. In order to achieve this, the SIP application of the ngHLR has been enhanced to return CAMEL information. To make use of this feature, the following parameters must be configured in the system:

- The IsCamelInfoIncluded parameter has been implemented in the RedirectConfig entity to enable (ON) or disable (OFF) this feature. In the case where this flag is set to OFF, the Tekelec ngHLR never adds the CAMEL data in the 30x responses. For additional information, such as the CAMEL data, to be included in the 30x response, the IsAdditionalInfoEnabled parameter must also be enabled (ON).

The configuration of these parameters can be viewed from the WebCI.

Upon receiving a `SIP INVITE` for a subscriber with both the SIP and GSM profile, the Tekelec ngHLR now behaves as follows depending on the situation:

- returns a `SIP INVITE` response that includes the subscriber's CAMEL data in the case where the following conditions are met:
  - The IsCamelInfoIncluded and IsAdditionalInfoEnabled parameters are all set to ON in the RedirectConfig entity.
  - The subscriber has CAMEL Data provisioned.
  - The subscriber has T-CSI CAMEL services provisioned and active.
  - The subscriber has T-CSI Terminating Attempt Authorized provisioned.

  If these conditions are met, the CAMEL information is returned in the body of the following SIP INVITE responses:
  - 480 (in the case where the subscriber has no MSRN or CFN)
  - 30x (in the case where the subscriber has MSRN and a CFN)
- returns a `SIP INVITE` response that doesn't include the subscriber's CAMEL data in the case where the conditions above are not met.

In the case where the conditions are met for the Tekelec ngHLR to return the T-CSI information of a subscriber in the `SIP INVITE` response, the T-CSI information will be included in the AdditionalInfo section of the message's body, as follows:

```
SIP/2.0 302 Moved Temporarily
From: <from details>
To: <to details>
Contact: <returned SIP contact>
Content-Disposition: render; handling="optional"
Content-Type: application/xml; charset="utf-8"
Content-Length: <length of message body in octets>
<?xml version='1.0' encoding='UTF-8'?>
<AdditionalInfo>
   <TCSIProvisioned>
      <camelCapabilityHandling>3</camelCapabilityHandling>
      <TBcsmCamelTDPData>
         <tBcsmTriggerDetectionPoint>12</tBcsmTriggerDetectionPoint>
         <serviceKey>23333333</serviceKey>
         <gsmSCF-Address>15634115555</gsmSCFAddress>
         <defaultCallHandling>0</defaultCallHandling>
      </TBcsmCamelTDPData>
   </TCSIProvisioned>
</AdditionalInfo>
```

For more information on the RedirectConfig entity and the IsCamelInfoIncluded parameter, refer to the "SIP Redirect Server" section of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to view this configuration parameter, refer to the "Configuring the SIP Redirect" section of the *SDM System Configuration - User Guide*.

SIP Redirection Override

With the implementation of this feature, a "redirection override" capability has been added to the SIP Redirection server. This provides an easy way for the operator to use the SIP Redirection Server for several functionalities, such as for the unconditional call forwarding (CFU) and local number portability.

With this feature, the operator can provision one or several "permanent redirection" contact URIs for each Address Of Record (AoR). When such URIs are provisioned (and the AOR attribute IsRedirectionOverrideActive is set to ON), the SIP Redirection server ignores any other call logic and immediately replies with the `302/300` message redirecting the `INVITE` to the provisioned contacts.

In order to achieve this, the following updates have been made in the Tekelec ngHLR's database and can be provisioned by the operator from the SDM interfaces:

- The IsRedirectionOverrideActive parameter has been added to the AddressOfRecord entity in order to allow the operator to turn On/Off this redirection override feature. Note that this feature is turned Off by default.
- The SipRedirectionOverride entity has been added in order to allow the operator to provision up to 10 "permanent redirection" contact URIs for a specific AoR.

In addition, two new counters have been added in order to count the number of times SIP INVITE 300 and 302 messages are redirected:

- RedirectOverrideSuccess300
- RedirectOverrideSuccess302

The Tekelec ngHLR's SIP Redirection Server behaves as follows on the reception of a SIP INVITE message for a given AoR:

- If the RedirectionOverrideActive flag is set to "1(On)" and at least one redirection URI is provisioned in the SipRedirectionOverride entity, then the Tekelec ngHLR's SIP Redirection server responds with a 302/300 message containing the redirection URI(s).
- If the RedirectionOverrideActive flag is set to "0(Off)" or if no redirection URI(s) have been provisioned in the SipRedirectionOverride entity for this AoR, then the Tekelec ngHLR proceeds with normal SIP INVITE processing logic.

Note: If at least one "permanent redirection" contact URI cannot be parsed into a contact (invalid URI) a 500 error will be sent back in response to the INVITE received.

For more information on the AddressOfRecord and on the SipRedirectionOverride entities, refer to the "AddressOfRecord" section in the SIP chapter of the *SDM Subscriber Provisioning-Reference Manual*. For step-by-step instructions on how to provision SIP Subscriber profiles with AddressOfRecords and "permanent redirection" contact URIs using XML files, refer to the "Examples of XML files for Subscriber Provisioning" chapter of the *SDM Subscriber Provisioning - User Guide*.

For step-by-step instructions on how to troubleshoot a SIP Subscriber profile with AddressOfRecords and "permanent redirection" contact URIs using the WebCI, refer to the "Viewing/Editing SIP Subscriber Profiles" section of the *SDM Monitoring, Maintaining, and Troubleshooting - User Guide*. For more information on the counters implemented in this feature, refer to the *SDM Performance Measurements* document.

Sequential ringing

A q-value can be set for each AOR defined for SIP Redirection Override. This indicates the order in which the devices must be reached (simultaneous or sequential ringing). This value can be set for each AOR defined in the SipRedirectionOverride entity. The Network Operator can set the SipRedirectionOverride entity's 'Qvalue' parameter to any value between '0' and '1' ('1' being the highest priority).

Improved SIP Traffic Distribution

This feature allows an easier distribution of `SIP INVITE` message processing on a system with more than 2 blades. In other words, it introduces a new way to distribute SIP INVITE traffic to many SIP Redirect servers all working in parallel on different blades

When using the Tekelec ngHLR's SIP Redirect server functionality, an HLR service with the SIP application enabled can run on each blade (2, 4, 8 or 12 blades) with only two of these instances using the SIP Stack's proxy to receive incoming messages from the external SIP UA Client Application node. These two proxies redirect in a round-robin manner the `SIP INVITE` messages to either the SIP Redirect server running on its own blade or on one of the other blades.

This deployment allows easier distribution of SIP INVITE traffic to each blade's SIP Redirect server while only using two external IP addresses to receive traffic.

The following has been added to the Tekelec ngHLR's database in order to allow this deployment to be configured:

- The IsLoadBalancingProxyEnabled parameter has been added to the SipServerConfig entity to allow to dynamically enable/disable this feature. Note that the redirection of SIP INVITE traffic to several SIP Redirection servers using the SIP Stack's proxy is by default disabled.

The MaxLoadBalancingProxyCoreObjects parameter has been added to the SipServerConfig entity to allow the operator to set the maximum of SIP INVITE messages (up to 10000) that can be simultaneously proxied by the SIP Stack at one given moment by one single SIP Stack.

Note: When using the deployment proposed in this feature, more CPU and memory will be used on the blades running the HLR service due to the additional use of the SIP Stack's proxy logic. Moreover, at least one of the two blades that receives the SIP INVITE traffic from the external SIP UA Client Application node must be up and running in order to be able to proxy and process the traffic.

For more details on these new parameters and the SIP Configuration entities, refer to the "SIP Configuration" section of the *SDM System Configuration-Reference Manual*. For instructions on how to provision this feature from the WebCI, refer to the "SIP Application Configuration" section of the *SDM System Configuration-User Guide*.

SIP Overload Control

This feature has been implemented in order to control the internal traffic between the SIP process and the HLR process when the HLR service is in overload state and can no longer respond to requests coming from the SIP process.

In order to achieve this, the following protection mechanism has been implemented:

- After the current number of pending HLR requests exceeds the value configured for the MaxPendingHlrRequests parameter, all the incoming `SIP INVITE` messages are aborted and a 486 "`Busy Here`" error message is sent back to prevent a SIP Overload. When this situation occurs,

the following new alarm is generated in order to notify the operator that the maximum pending HLR requests has been reached and that the next requests will be discarded:

- MaxPendingHlrRequestsReached (Alarm Id: `8042`)

The following new parameters have been added to the RedirectConfig table and can be viewed from the WebCI:

- The MaxPendingHlrRequests parameter, which is set to 100 000 HLR requests by default. Upon the operator's request, this value can be changed by Tekelec's *Customer Care Center* in order to be more accurate with the operator's traffic model.
- The MaxPendingHlrRequestsThreshold parameter is set to 50% by default and can also be modified. When this threshold is reached, the following alarm is raised to notify the operator:
  - MaxPendingHlrRequestsThresholdReached (Alarm Id: `8044`)

Note: The alarms are not updated in real time when the related configuration parameters are modified but rather when the next SIP INVITE request for a subscriber provisioned with a GSM profile comes in.

For more information on the RedirectConfig System Configuration - Reference Manual entity and its configuration parameters, refer to *SIP Redirect Server*. For step-by-step instructions on how to view the configuration parameters, refer to the "Configuring the SIP Redirect" section of the *SDM System Configuration - User Guide*.

SIP NP support for AOR ranges

The SIP NP Support for AOR Ranges feature offers two functionalities:

- Redirect SIP INVITE requests for Address of Record (AOR) ranges
- Include full routing numbers in SIP response

The SIP NP Support for AOR Ranges feature allows the operator to define groups or ranges of users using prefixes and provision information to redirect SIP INVITE requests that are sent to any of these users. A user belonging to a range of users does not need to be provisioned individually in the system.

If this feature is enabled and the user part of the To header URI matches a provisioned prefix range, the 302 message response returns the Contact information provisioned in the range definition.

The SIP NP Support for AOR Ranges feature also allows the operator to provision the RuleId to retrieve the full routing number from the MNP server and return it in the Contact URI header of the 302 message response.

If this feature is enabled and the user part of the To header URI matches a provisioned prefix range, and if the range is provisioned to use MNP routing rule, the 302 message response returns a URI with the full routing number in the user part of the Contact header. In addition to a fixed routing number (RN), the return results can have these formats: CC RN MSN.

If the full routing number retrieval fails, the system returns the SIP response 404 Not Found.

The SIP NP Support for AOR Ranges feature impacts the SIP Redirection Override feature as well as the VoIP DN Allocation feature. Upon reception of a SIP Invite message, if the user has redirection override records, the SIP Redirection Override feature is processed first, If the VoIP DN Allocation feature is enabled, it is executed next.

SIP NP AOR redirection occurs last, and only when SIP Redirection Override is disabled or no redirect override contacts are provisioned. If a SIP Registration binding or an HLR MSRN is found, the

302-response returns their information. SIP NP AOR redirection, is executed only when no other contacts have been found.

Configuration

The operator can provision this feature from the CLI and WebCI using these tables and attributes:

- Redirect
  - IsSipRangeSupportEnabled

This field allows the Network Operator to enable/disable the feature

- NipAorUserRangePrefix:
  - UserRangePrefix

This field allows the Network Operator to assign the prefixes to a range of users.

- isMNPRoutingRuleUsed

This field allows the Network Operator to specify whether the MNP routing rules shall be used (On/Off)

- Ruled

This field allows the Network Operator to define the MNP routing rule to use.

- Contact

This field allows the Network Operator to define the content of the Contact header to be returned in the 302 redirection when the MNP routing rules shall not be used (Off).

Counters

A new counter identifies the number of SIP INVITEs redirected with NP AOR User Range Prefix contact (302). Refer to the latest *SDM Performance Measurements* for more details on this counter.

Counter name	**Description**
RedirectNpAorUserRangePrefixSuccess302	Number of INVITE redirected with NP AOR User Range Prefix contact (302)

Error Messages

Locate the error messages in the SIP Provisioning Error Notifications table in the *Monitoring, Maintaining, and Troubleshooting – Reference Manual*.

15041	InvalidNpAorUserRangePrefix	Invalid Prefix received for feature NP AOR user range.
15042	InvalidNpAorUserRangeContact	Invalid Contact received for feature NP AOR user range.
15043	InvalidNpAorUserRangeRuleId	Invalid RuleId received for feature NP AOR user range.

15044	InvalidNpAorUserRangeIsMNPRule	Invalid MNP Routing Config received for feature NP AOR user range.
15045	InvalidUpdateNpAorUserRangeIsMNPUsed	NP AOR user range parameter 'isMNPRoutingRuleUsed' cannot be updated for an existing prefix.

GSM Registration Agent

In the SIP-anchored FMC + GSM registration agent model, the primary network registrar is located in the SIP domain (this can be either an IMS network or a pre-IMS SIP network). In this case, the Tekelec ngHLR acts as a gateway between the GSM mobile network and the SIP network. The responsibility of the Tekelec ngHLR is to provide the IMS network or the pre-IMS SIP network with contact information for GSM mobile subscribers.

This is achieved by performing a SIP Register/Deregister for each GSM subscriber, thereby making non-SIP GSM devices appear to be valid SIP endpoints, with SIP contact information. The GSM registration agent is the element used to register GSM subscribers with an external SIP registrar. The GSM registration agent relies on the SIP Redirect Server integrated in the Tekelec ngHLR to process incoming Invite requests. To achieve this, the registration contact info provided is the SIP Redirect Server contact Info.

SIP UA authentication with http-Digest

The implementation of the "SIP UA authentication with http-Digest" feature enables the SIP User Agent (GSM registration Agent) functionality of the Tekelec ngHLR to handle a REGISTER message sequence with authentication credentials. With this feature, when the SIP UA sends a REGISTER message to the external SIP Registrar (located in the operator's network), which challenges back with a 401 (Unauthorized) response, the SIP UA is capable to respond back by sending another REGISTER message that includes the user's AOR authentication credentials (authentication username and authentication password). The SIP UA uses the http-Digest authentication algorithms to support authentication with an external SIP Registrar. More precisely, it supports the MD5 algorithm and a qop (quality of protection) "auth", as defined in the http-Digest RFC 2617.

SIP UA 3GPP Gm Interface phase 1

The implementation of the "SIP UA 3GPP Gm Interface phase 1" feature has added the possibility for the GSM registration Agent (SIP User Agent) to include, as per the 3GPP TS 24.229, the following 3GPP "IMS specific" headers in a REGISTER message:

- IMS Header Required
  - P-Access-Network-Info
  - Authorization
- Path Header
  - Path
- Username in Contact Header
  - Contact

- Username is Phone Number
  - To
  - Contact

The GSM Registration Agent (SIP UA) includes or not these "IMS specific" headers in the REGISTER message depending on system level configuration settings.

The SIP UA can be configured with the "IMS specific" headers that need to be included in a REGISTER message at system startup. The configuration of the following parameters can be viewed through the WebCI or CLI:

- The "IsImsHeaderRequired", "IsUsernameSetInContactHeader", "IsUsernamePhoneNumber" and "IsPathHeaderRequired" parameters in the SipUaConfig entity. At system startup, these parameters can be set to On/Off to include or not the corresponding "IMS specific" headers in the REGISTER message.
- "PathHeaderValue" parameter in the SipUaRegisterConfig entity. At system startup, this parameter is configured with the path value when the "IsPathHeaderRequired" parameter is set to "ON".

For more details on these parameters implemented with the "SIP UA 3GPP Gm Interface phase 1" feature, refer to the "User Agent" section of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to view the configuration of these parameters, refer to the "Configuring the SIP User Agent" section of the *SDM System Configuration - User Guide*.

SIP Diversion header

When using the Cisco PGW, the 300 and 302 responses are recognized for call routing. The responses can also be used to trigger IN queries to an SCP. However, with the Tekelec ngHLR's current response format, the Cisco PGW creates an IN query with the original A party and the MSRN (or call forwarding number) as the B party. This means the SCP does not have the original called party for service execution.

This feature adds the SIP "Diversion" header to 300 and 302 responses returned by the Tekelec ngHLR. The Cisco PGW uses this header to set the B party correctly in the IN query

This feature allows the Cisco PGW to be used as a GMSC for call routing with INAP services.

The IsDiversionHeaderIncluded parameter has been added to the RedirectConfig entity and allows the Network Operator to configure the Redirect Server to include or not the Diversion header in the 300 and 302 responses. The ON/OFF redirect setting for the inclusion or not of this header is dynamic and can be set through the SDM CLI or WebCI.

When the IsDiversionHeaderIncluded parameter is set to '1' (On), the Redirect Server includes the Diversion header in the 30x message when it contains at least one GSM contact.

Moreover, the Tekelec ngHLR's Redirect Server has been configured to set the Diversion header's parameters as follows:

- The 'reason' parameter for CFU scenarios is set to "unconditional:.
- The 'reason' parameter for CFNRc scenarios is set to "user-busy".
- The 'reason' parameter is set to "follow-me" when an MSRN is returned.
- For all scenarios, the counter parameter is set to "1".
- For all scenarios, the screen parameter is set to "yes".

For more details on the "IsDiversionHeaderIncluded" parameter, refer to the RedirectConfig entity in the "SIP Redirect Server" section of the *SDM System Configuration - Reference Manual*. For instructions

on how to provision this parameter, refer to the "Configuring the SIP Redirect" section of the *SDM System Configuration - User Guide*.

VoIP DN allocation enhancements phase 1

When a call is redirected from GSM to SIP using a MAP-SRI sequence, the Tekelec ngHLR returns a statically assigned VoIP DN as the MSRN in the `SRI-ACK` message. This allows the G-MSC to route the call to the appropriate Gateway, which can then retrieve from its database the correct AOR that will be used in the SIP INVITE in order to communicate with the user. In order to reduce the need for the Network Operator to maintain identical databases (AOR-VoIP DNs) in the Tekelec ngHLR and in the Gateways, the following enhancement has been implemented in the Tekelec ngHLR:

- The Tekelec ngHLR can now support `SIP INVITE` messages with a VoIP DN as the 'User' part of the AOR URI.
- The Tekelec ngHLR's SIP INVITE handling logic has been enhanced to be able to compare the 'User' part of the SIP INVITE's AOR URI with the VoIP DNs stored in its database in the cases where the AOR itself doesn't match any of the AORs stored in its database.
    - In other words, when receiving a `SIP INVITE`, the SIP Server performs an AOR Reverse Search by searching the AOR through the list provisioned in the system's database by using the URI received in the 'To' header of the message. In the case where the AOR is not found, the SIP Server has the capability to perform a Reverse Search of the AoR, which consists in searching through the database's list of AORs Directory Number, using the user part only of the `SIP URI` received.
    - When a match is found, the Tekelec ngHLR returns a 30x message with the corresponding AOR and in the cases where no match is found, the Tekelec ngHLR returns a 40x message.

With this new behavior, instead of searching through its database in order to obtain the user's AOR, the Network Operator's Gateway can now send to the Tekelec ngHLR a `SIP INVITE` with an AOR URI that includes a VoIP DN as the 'User' part.

Moreover, the following new counters have been implemented:

- RedirectVoipDnUriSuccess302: This counter counts the number of `INVITE` redirected to VoIP DN AOR.
- InviteVoipDnError500: This counter counts the number of `VoIP DN INVITE` answered with 500.

For more details on these counters, refer to the *SDM Performance Measurements* document.

SIP over TLS transport protocol

Enhancements have been made to the SIP Server (SIP Registrar, SIP User Agent, SIP Redirect) in order to support the TLS transport protocol, which encrypts the SIP packets over the TCP transport protocol in order to provide security for the SIP traffic. For the SIP traffic to be able to run over TLS, the TlsSupport must be enabled and the SIP Server must be configured with the following:

- For Registrar and Redirect:
    - Provisioned AOR with 'sips' scheme
- For the UA the following configuration is necessary:
    - SipUaConfig::OutboundProxyTransport = 3 (TLS)
    - SipUaRegisterConfig::RequestUriScheme = 2 (sips)

To support the TLS transport protocol, the following entities, fields and operations have been implemented:

- The SipServerTlsConfig entity has been implemented to allow the Network Operator to view the TLS configuration information, loaded by Tekelec at startup.

  The TLS Support is by default disabled. Call the Tekelec *Customer Care Center* to edit TLS configuration and enable the TLS Support. Take note that changes made to the TLS configuration can be edited dynamically during running-time of the system with the exception of changes made to the TLS Support activation status and to the maximum number of sessions opened simultaneously, which require a restart of the HLR service for the changes to take effect.
- The following operations have been implemented:
  - LoadPEMFiles(): this operation allows the Network Operator to load a TLS certificate and private key from the following well known PEM files onto the database:

    `/tmp/cacert.pem and /tmp/cakey.pem`
  - DisplayCertificate(): this operation displays the details of the Certificate.

Note: In this release, multiple certificates are not supported, only one certificate and one private key can be loaded. In order to modify these, contact the Tekelec *Customer Care Center*.

- The following value has been added to the SipUaConfig's OutboundProxyTransport parameter: 3 (TLS)
- Error messages have also been added:
  - `MultipleSipTlsCertPrivKeyNotAllowed`
  - `TlsInvalidAttribute`
  - `InvalidTlsCertificate`
  - `InvalidTlsPrivateKey`
  - `MandatoryTlsAttributeMissing`

    Refer to the "Error messages" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual* for more details on these error messages.

In addition to these enhancements, the Sips Port can now be dynamically configurable and modified from the WebCI.

For more details on the SipServerTlsConfig entity and on the LoadPEMFiles() and DisplayCertificate() operations, refer to the "SIP entities" chapter of the *SDM System Configuration - Reference Manual*.

For instructions on how to load PEM files and display Certificate content from the WebCI, refer to the "Viewing/Editing SIP Server Configuration" section of the *SDM System Configuration - User Guide*.

SRI Router

The purpose of this feature is to allow mobile terminated calls from the cellular domain to be routed to a Telephony Application Server (TAS) when a subscriber is registered in the SIP/IMS domain.

With the implementation of this feature, the SIP Registrar can support registrations from a 3rd party, more specifically it allows the SIP Registrar to receive `SIP REGISTER` messages from a TAS node. Upon registration, the system generates a SIP Registration Binding with the ID of the TAS (TasId) the `SIP REGISTER` message comes from.

When a `MAP SRI` message is received, the SDM ngHLR tries to find the TasId in the SIP Registration bindings with the MSISDN received from the `SRI` message. The key that links the MSISDN with the SIP Registration binding is the SubscriptionID. If the TasId returned from the database request is not '0' (0 means there is a registration that is not a 3rd party registration), the SDM ngHLR treats the subscriber as being SIP registered from a 3rd party. At this point, the SDM ngHLR relays the SRI message (modifying the CdPA Gt and Tt) based on the TAS information (TAS GT address, Tt) configured for the TasId stored in the subscriber's registration binding. If the subscriber is not SIP registered, the SDM ngHLR returns the SRI message to the GSM network with a different Translation Type.

Hereunder are call flows that show the message handling in the case where a subscriber is SIP registered and in the case where the subscriber is not SIP registered.

The REGISTER/DE-REGISTER call flow is depicted in the diagram below.

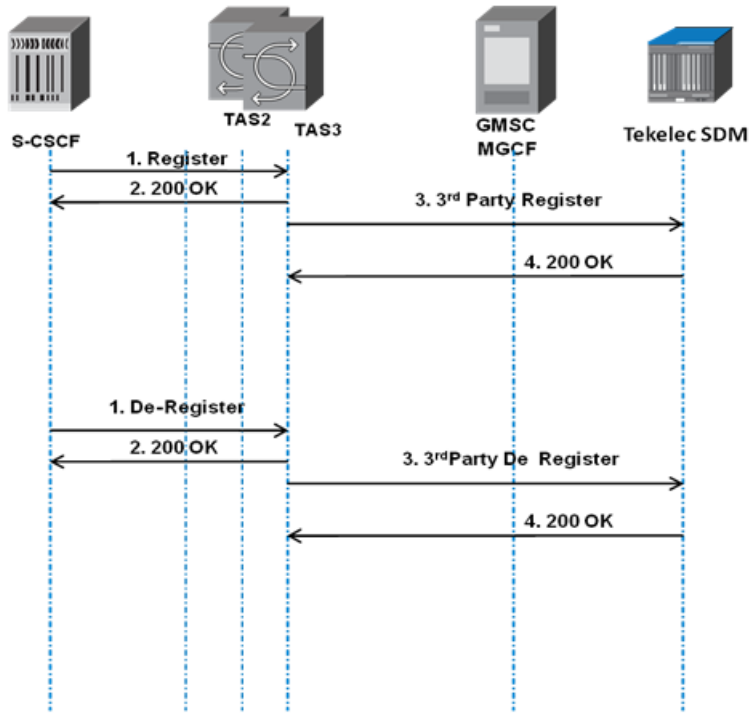


Figure 58: Register/De-register call flow in the IMS Domain for 3rd party registration from TAS node.

The SRI message call flow for a subscriber that is SIP registered is depicted in the diagram below. In this case, the SDM ngHLR relays the SRI message to the corresponding TAS.

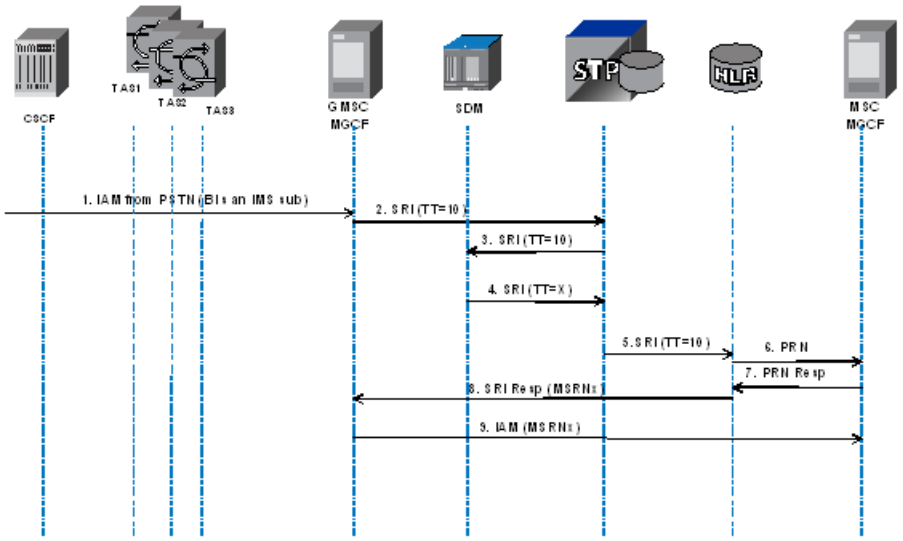


Figure 59: SRI message routing call flow in the IMS Domain for a 3rd party SIP registered subscriber.

Note: This diagram is for illustration only. Networks may be configured differently. Ack messages will pass through the STP.

The SRI message call flow for a subscriber that is not SIP registered is depicted in the diagram below. In this case, the SDM ngHLR returns the SRI message to the GSM network with the same Gt but with a possible different Translation Type.

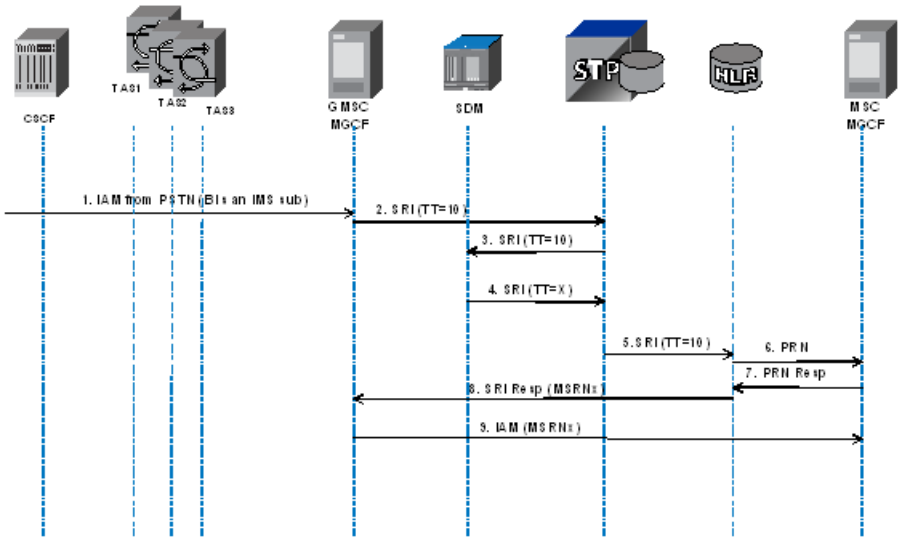


Figure 60: SRI message routing call flow in the IMS Domain for a subscriber with no 3rd party SIP registration.

Note: This diagram is for illustration only. Networks may be configured differently. Ack messages will pass through the STP.

SIP Server functionality

The SIP Server functionality introduced by this feature mainly consists in the implementation of the following capabilities:

- Support registrations from a 3rd party, more specifically it allows the SIP Registrar to receive `SIP REGISTER` messages from a TAS node.
- Create SIP Registration Bindings for 3rd party registrations with a TasId.

This SIP functionality is available by default when the SIP Registrar server is enabled, it is invoked automatically when a 3rd party registration is detected at runtime.

It is important to note that this feature introduces limited support for 3rd party registrations as follows:

When the "to" and the "from" headers are different, the following logic is applied:

1. The FROM URI user part is NOT mandatory. If a user part is received, it is ignored.
2. The 3rd party REGISTER is NOT rejected if the host part of the "from" header (i.e., TAS FQDN) is provisioned in the SipTasGt entity.
3. If the 3rd party IMS REGISTER is detected but the TAS FQDN is not configured, the `SIP REGISTER` request is rejected with a 404 error message.

If the "to" and the "from" headers are equal, normal SIP Registration processing applies (SIP Registration process without the 'SRI Router' feature).

A user can have a single third party registration binding (i.e., a maximum of one registration with a non-zero TasId). If a re-registration for a user occurs from a different TAS (i.e., a different "from" header), the Registration Binding is overwritten since it is from the same user (i.e., the same "to" header). A RegistrationBinding is deleted when a DE-REGISTER is received or when the RegistrationBinding cleanup is activated and the RegistrationBinding is expired (please refer to the 'Registration Binding cleanup' section for more details).

HLR Server functionality

The HLR Server functionality introduced in this feature mainly consists of an addition to the MAP SRI process mechanism to relay the SRI message based on the TAS ID (TasId) of the 3rd party SIP registration bindings.

The HLR Server functionality introduced in this feature is initially unavailable and the Tekelec Customer Support Team must be contacted in order to make it available. Once available, the Network Operator can activate/deactivate it by performing the ActivateFeature()/DeactivateFeature() operation with the Feature ID 24 for SriRouting. For more details on this operation, refer to the 'HLR Operations' section of the *SDM System Configuration - Reference Manual*.

Note: The HLR Server processes the MAP SRI message using the process specifically implemented for the MNP and SSR features, before verifying the activation status of the 'SRI Router' feature. Based on this, it then continues to process the MAP SRI message by performing either the normal MAP process (if SriRouting activation status 'disabled') or the MAP process as implemented for the 'SRI Router' feature (if SriRouting activation status 'enabled'). In the case where the 'SRI Router' feature is enabled, the SDM ngHLR either relays the MAP SRI message back to the GSM network with the same Gt but with a possible different Translation Type (if the subscriber is not 3rd party SIP registered: TasId=0) or relays the MAP SRI message to the corresponding TAS (if the subscriber is 3rd party SIP registered: TasId ≠ 0), by modifying the CdPA Gt and/or Tt with the TAS's Gt and Tt.

The Registration Binding cleanup (expiration) affects the HLR Server's database request to find the TasId. If the RegistrarConfig entity's 'IsExpiryTimestampSet' flag is set to '1' (Registration Binding cleanup enabled), the SDM HLR Server tries to find the TasId in SIP registration bindings, but only if the 'RegistrationExpiryTime' is greater than the current time. If the 'IsExpiryTimestampSet' flag is set to '0' (Registration Binding cleanup disabled), the SDM HLR Server doesn't verify the 'RegistrationExpiryTime'. For more details on the Registration Binding cleanup mechanism, refer to the next section "Registration Binding cleanup" of this document.

To achieve this, the following entities/parameters have been implemented and can be configured by the Network Operator either through the WebCI, CLI or XML interfaces:

- 'SipTasGt' entity. This entity allows to define a TAS GT address and map it to the SIP registration binding's TAS ID ('TasId' parameter) in the context of a 3rd party registration. It also allows to set the 'OverrideTt' flag, which indicates to the HLR Server whether to modify or not the Tt when relaying the SRI message.
- 'SriRouting' activation flag in the HlrConfig entity. This flag allows to enable/disable the 'SRI Router' feature for the SDM ngHLR.
- 'TasId' parameter in the SIP RegistrationBinding entity. The TasId is generated by the system, by retrieving the ID of the TAS node from which the SIP REGISTER message came from. 3rd party registrations stored in the SIP REGISTRAR are identified by a TasId.

In addition to this, the following counters and alarms have been implemented in the context of this feature:

- Counters: RegisterImsrTasNotFound, SriRoutingSriReceived, SriRoutingSriRegistered, SriRoutingSriNotRegistered, SriRoutingSriNotFound, SriRoutingNonSri
- Alarms that inform when the feature has been activated/deactivated: `SriRoutingActivated` and `SriRoutingDeactivated`

For more details on these counters, please refer to the *SDM Performance Measurements* document. For more details on these alarms, please refer to the *SDM Alarm Dictionary*.

For the SDM system to be able to perform all the functionalities implemented for this feature, you must ensure that the following is configured in the SDM system:

- The SIP Server and HLR Server must both be configured and capable of actively running traffic.
- The SIP RegistrarConfig entity. For optimum performance, here is the recommended configuration (contact the Tekelec Customer Care Center for more details or further assistance):
  - **MaxContactsPerAor(1)**

    If the system is used only for third party registrations, this parameter can be set to 1. In fact, contacts are not stored for third party registrations.
  - **MaxRegClients (64000)**

    The recommended value is 64000 in order to support burst traffic at 2000 TPS over UDP (2000 TPS * 32 s = 64000 simultaneous reg objects).
  - **IsExpiryTimestampSet (0/1)**

    Set depending on whether the client will send re-registrations.
  - **IsRegistrationCleanupEnabled (0)**

    If this flag is enabled, the cleanup needs to run during low traffic hours.
  - **RegistrationBindingCleanupTime**

    This parameter should be set based on the traffic model. If, for example, the IMSR REGISTRAR runs in Canada and at 2a.m. the traffic is usually lower, given the time zone (i.e. +5 hours) this parameter should be set to 07:00.
  - **MinRegistrationDuration**

    This parameter should be set to the minimum value of the contact expiration time in the SIP REGISTER request.

- This feature requires the following entities to be provisioned at a minimum for each subscriber:
  - Subscription
  - AddressOfRecord
  - MsIsdn
    - For a subscriber that only requires the SRI message relay functionality, it is not necessary to provision a MSISDN-IMSI association (in the MsIsdnImsiProfileAssociation entity), and only an MsIsdn is required.
- Both of the following SIP domains must be provisioned in the 'Domain' entity before running SIP traffic:
  - Request-URI domain
  - TO URI domain

Contact the Tekelec Customer Care Center for further assistance to provision this since the Hlr service needs to be restarted for any changes to be committed. A specific maintenance procedure is used to ensure there is no loss of service.

- The 'SipTasGt' entity must be provisioned with the configuration data of each TAS from whom the SIP Registrar can accept SIP REGISTER messages from.
- The HlrConfig entity's 'SriRouting' flag must be Activated.
- For SS7 provisioning, an outgoing route must be defined for the Gt/Tt combination.

Contact the Tekelec Customer Care Center for further assistance.

For more information on the entities/parameters implemented for this feature, refer to the 'HLR Configuration' and 'SIP Configuration' sections of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision/troubleshoot these entities/parameters from the WebCI, refer to the 'Configuring the HLR' and 'Viewing/Editing SIP TAS Configuration for 3rd party Registration' sections of the *SDM System Configuration - User Guide*.

Registration Binding cleanup

The Registration Binding cleanup mechanism has been implemented in order to delete expired registration bindings and ultimately increase the performance of the system. The Network Operator can have full control on the activation of this mechanism, its execution time and on the enabled/disabled status of the expiry timestamp of the registration bindings. To achieve this, the Network Operator can provision the SIP RegistrarConfig entity's following parameters from the CLI, WebCI or XML interfaces:

- The 'IsExpiryTimestampSet' parameter, which allows to enable/disable the Registration Expiry Timestamp (field set in the Registration Bindings upon registration of the subscriber).

  If the 'IsExpiryTimestampSet' parameter is disabled (set to '0'), the registration expiry timestamp will be set to '0000-00-00 00:00:00'. This means that the registration binding will never expire and a re-registration is not required from the client or from the main Registrar server, if the registration cleanup mechanism is not enabled.

  If the 'IsExpiryTimestampSet' parameter is enabled (set to '1'), the expiry timestamp will be set to the time when the binding will expire (current timestamp value + RegistrationExpiryTime value).
- The 'IsRegistrationCleanupEnabled' parameter, which allows to dynamically enable/disable the Registration Binding cleanup mechanism. If disabled, the Registration Binding cleanup mechanism

is not performed and if enabled, it is performed once a day at the time set in the 'RegistrationBindingCleanupTime'. By default, it is disabled.

- The 'RegistrationBindingCleanupTime' parameter, which allows to set the GMT of the day the RegistrationBinding cleanup must be performed. By default, it is set to (00:00).

For more details on these parameters, refer to the "SIP Registrar" section of the *SDM System Configuration - Reference Manual*. For instructions on how to provision the Registration Binding cleanup mechanism from the WebCI, refer to the "Viewing/Editing SIP Registrar configuration" section of the *SDM System Configuration - User Guide*.

IMS-HSS Features

The IMS-HSS 3GPP standard functionalities

Support of Cx/Sh (HSS module) and Dx/Dh (SLF module)

For the IMS-HSS, the DIAMETER Cx and Sh applications provide simple interfaces that allow access to the HSS module and the DIAMETER Dx and Dh applications provide simple interfaces that allow access to the SLF functionality of the HSS module. The IMS-HSS is designed as per the following standards: TS 3GPP 29.228, TS 3GPP 29.229, TS 3GPP 29.328, TS 3GPP 29.329, TS 3GPP 23.380. The IMS-HSS is now compliant with the 3GPP Release 7.

The I-CSCF, S-CSCF and AS are Diameter Multimedia clients which connect to the IMS-HSS. Incoming messages from S-CSCF/I-CSCF/AS are processed by the IMS-HSS, where the IMS-HSS acts as a server regarding Diameter Protocol. The IMS-HSS can send Cx/Dx and Sh/Dh messages in response to an invocation from a CSCF or an AS but can also invoke procedures to the CSCF or AS in order to inform them of changes in data.

The IMS-HSS is notified from Diameter Stack about incoming messages and has to:

- Check that the required information can be provided
- Interact with the database to retrieve necessary information to compute the answer
- Compute an answer with corresponding status (`SUCCESS` or `FAILED`) and fill corresponding information in message if success.

The IMS-HSS is always located in the home network and communicates with the Call Session Control Function (CSCF) and the Application Server (AS) within the Session and Database Layer of the IMS network. It hosts subscriber related information in support of IMS session establishment for a given subscriber by solving authentication, authorization, address resolution, subscriber location dependencies, and distribution of subscriber's service related information. Moreover, the IMS-HSS can provide routing information to the CSCF and AS with the Subscription Locator Function functionality.

The key parameters for user identification on IMS network are private user identity and public user identity. The private user identity is the parameter that is stored in the IMS-HSS as a permanent subscriber data and takes the form of a Network Access Identifier (NAI). It is not known publicly nor by the user and is used by the network to determine the access allowance of the given user to the IMS network. The public user identity, on the other hand, is the parameter, which is used by the other subscribers on the network to address the subscriber holding public identity in a format that is known

publicly. The Public User Identity is stored in the IMS-HSS as a permanent subscriber data and takes the form of either a SIP URI or a tel URL.

It is possible to link multiple public identities to a single private identity with its own service profile associated to it. This makes it possible for a single service profile to be associated to multiple terminals and therefore to link several PublicId to a single PrivateId.

The IMS-HSS downloads user registration Profile into S-CSCFs with the Cx interface using the Diameter network. It communicates with the I-CSCF and S-CSCFs by exchanging Diameter messages. A P-CSCF(Proxy-Call Session Control Function) is a SIP proxy that is the first point of contact for the IMS terminal. The IMS User Equipment's registration is received by the P-CSCF in the visited network and then sent to the I-CSCF of the subscriber's home network in charge of finding the appropriate S-CSCF and providing the IMS-HSS the following information: the user's public and private identity and the P-CSCF network identifier.

The IMS-HSS is then in charge of verifying whether the user is registered already, and indicating whether the user is allowed in that P-CSCF network according to the User subscription and the operator's limitations/restrictions. Once the appropriate S-CSCF receives one of its subscriber's UE registrations, it is mainly responsible for all session management activities, for retrieving user profile and authentication information from the IMS-HSS and providing SIP routing.

The IMS-HSS uses the Cx interface and the SLF functionality (described in *Subscription Locator Function (SLF)*) of the IMS-HSS uses the Dx interface to provide the following operations to the CSCF:

- Location Management:
  - Registration and de-registration between the S-CSCF and the IMS-HSS (or SLF of the IMS-HSS).
  - Location retrieval operation.
- User Data Handling:
  - Download of user information into S-CSCF during registration and during system recovery
  - Update of user information and recovery mechanism.
  - User Authentication between the IMS-HSS (or SLF) and the S-CSCF.
- IMS CSCF Context Restoration.

In order to exchange all of this information, Cx messages are sent over the Diameter Base Protocol between the IMS-HSS and the CSCFs or in the case of a multi-HSS deployment, Dx messages are sent over the Diameter Base Protocol between the SLF functionality of the IMS-HSS and the CSCFs.

The IMS-HSS supports the following Cx/Dx messages:

- `UAR`: User-Authorization-Request (Code 300)
- `SAR`: Server-Assignment-Request (Code 301)
- `LIR` : Location-Information-Request (Code 302)
- `MAR`: Multimedia-Authentication-Request (Code 303)
- `RTR`: Registration-Termination-Request (Code 304)
- `PPR`: Push-Profile-Request (Code 305)

The UAR, SAR, LIR and RTR messages are Location Management Commands used over the Cx/Dx interfaces to check on multimedia access permission, roaming agreements and perform operations on User Public Identities. The MAR message is an Authentication procedure used over the Cx/Dx interfaces between the S-CSCF and the IMS-HSS or the SLF to compute the authentication between the end user and the home IMS network. Finally, the PPR message is a data handling procedure

initiated by the IMS-HSS to update user profile information and/or charging information in the S-CSCF.

For more details on Cx/Dx messages, refer to *Performance management*.

Within the home network, the IMS-HSS also communicates with the Application Server (AS) through the Diameter Sh interface and the SLF functionality (described in *Subscription Locator Function (SLF)*) of the IMS-HSS communicates with the AS through the Diameter Dh interface. When a user subscribes to a new service, it is provisioned by the operator in an Application Server. The AS stores some service data for a user in the IMS-HSS. Therefore, the IMS-HSS and the AS communicate together to exchange and update service related data for users. More precisely, the AS downloads the data needed for providing service from the IMS-HSS and receives updates from the IMS-HSS when user data is updated by subscribing to notifications from the IMS-HSS of changes in data. The AS can also decide to update user's service data.

The IMS-HSS uses the Sh interface and the SLF functionality (described in *Subscription Locator Function (SLF)*) of the IMS-HSS uses the Dh interface to provide the following operations to the Application Server:

- Data Handling Procedures:
  - Download of data from the IMS-HSS/SLF to an AS
  - Update of data in IMS-HSS/SLF
- Subscription/Notification Procedures:
  - AS subscription for IMS-HSS/SLF notification on change in data (The IMS-HSS can notify an AS of changes in data for which the AS previously had subscribed.)

In order to exchange all of this information, Sh messages are sent over the Diameter Base Protocol between the IMS-HSS and the AS and the Dh messages are sent between the SLF functionality of the IMS-HSS. The IMS-HSS supports the following Sh/Dh messages:

- `UDR /UDA`: User-Data-Request/Answer (Code 306)
- `PUR/PUA`: Profile-Update-Request/Answer (Code 307)
- `SNR/SNA`: Subscribe-Notifications-Request/Answer (Code 308)
- `PNR/PNA`: Push-Notification-Request/Answer (Code 309)

The UDR/UDA message is a Data Handling Command used over the Sh/Dh interfaces to read transparent and/or non-transparent data for a specified user from the IMS-HSS/SLF. The PUR/PUA message is also a Data Handling Command used over the Sh/Dh interfaces used to allow the AS to update transparent (repository) data stored at the IMS-HSS for a specified IMS Public User Identity or Public Service Identity and also to allow the AS to update the PSI Activation State of a Public Service Identity in the IMS-HSS. The SNR message is a Subscription/Notification Command used between the AS and the IMS-HSS. It is invoked by the AS to subscribe to Notifications for when particular transparent and/or non-transparent data for a specified IMS Public User Identity or Public Service Identity is updated, from the IMS-HSS. Finally, the PNR/PNA message is also a Subscription/Notification Command used between the IMS-HSS and the AS, but this time invoked by the IMS-HSS to inform the AS of changes in transparent and/or non-transparent data to which the AS has previously subscribed to receive Notifications for, using Sh-Subs-Notif (SNR message).

For more details on Sh/Dh messages, refer to *Performance management*.

Note: as part of being compliant with 3GPP Release 7, the IMS-HSS also supports the Notif-Eff feature.

Subscriber Location Function (SLF)

In the case where multi-HSS are deployed, the CSCF and AS Diameter peers do not have information on which IMS-HSS they need to communicate with regarding a subscriber. In such a case, the CSCF and AS would send their Diameter queries to a Subscription Locator Function (SLF) that is in charge of taking care of returning the name of the IMS-HSS hosting the subscriber.

The IMS-HSS provides the ability to configure and provision the Subscription Locator Function functionalities through the CLI or WebCI. In a multi-HSS deployment environment, the CSCF and AS send respectively Dx and Dh messages to the IMS-HSS with the SLF configured. The SLF functionality of the IMS-HSS will then be in charge to retrieve routing information from the database and adding an AVP in the response message to the Diameter peer by providing the name of the IMS-HSS hosting the subscriber.

When the CSCF and AS do not know which IMS-HSS holds the subscriber record, the CSCF sends Dx messages (UAR, SAR, MAR, LIR) to the SLF functionality of the IMS-HSS over the Diameter Dx interface and the SIP AS sends Dh messages (UDR, PUR, SNR) to the SLF functionality of the IMS-HSS over the Dh interface.

The Dx interface is similar to the Cx interface and the Dh interface is similar to the Sh interface, except the Dx and Dh interfaces communicate with the SLF

Support of UAR at 1st Registration

In UAR as defined by 3GPP, the Private Identity (PRID, in User-Name AVP) is mandatory, because any 3GPP-compliant REGISTER provides a Private Identity. In order to prevent the UAR from being rejected by the IMS-HSS 's Diameter Stack, in the case where the initial REGISTER does not provide any Private Identity (with the User-Name AVP missing), the UAR must carry a User-Name AVP with a reserved value.

This reserved value is "`unknown@unknown.invalid`" by default.

Moreover, it now follows a non-standard behavior in the case where no Private Identity is provided at first registration, which consists in ignoring the User-Name. In such situation, the IMS-HSS does not perform the following verifications:

- That the provided Private Identity exists;
- That the Private Identity is allowed to use the provided Public Identity (PUID);
- That the Private Identity is not blocked because of too many bad passwords entered.

On the other hand, the IMS-HSS is still able to check that the PUID is not a PSI.

In the case of a classic SIP UE (as per the IETF profile), the IMS-HSS verifies the Private Identity's (PRID) existence and the PRID/PUID's association during the handling of the second, authenticated REGISTER.

Support of LIR messages Release 7

The IMS-HSS now supports the LIR messages Release 7. This means that the IMS-HSS does not compile the LIA content only based on user state, but also if we are in an optimization case or not. The optimization case is when a user is UNREGISTERED or NOT_REGISTERED (regardless if an S-CSCF is assigned or not), he/she has no Initial Filter Criteria for unregistered state and we are on the terminating side.

The IMS-HSS responds to a `LIR` message for a user in an optimization case, with a specific error Result-Code (`ERROR_IDENTITY_NOT_REGISTERED`) in LIA that leads the I-CSCF to directly reject the `INVITE` request with a `SIP 480 Temporarily Unavailable` response, without involving the S-CSCF. All of this can happen regardless if a S-CSCF is assigned to the IMS Subscription or not.

Shared Initial Filter Criteria (Shared iFC)

In the IMS-HSS, the Shared Initial Filter Criteria feature allows for the Initial Filter Criteria of different Service Profiles to be shared.

In order to be able to use this feature, both the IMS-HSS and the S-CSCF should support it. However, SharedIFCs can be defined in the IMS-HSS even if the S-CSCF doesn't support SharedIFCs. When the SAR is sent, if the S-CSCF doesn't support the SharedIFCs, the IMS-HSS sends the complete IFC instead of the unique identifier which defines the SharedIFC.

For the IMS-HSS, the Shared Initial Filter Criteria feature can be provisioned through the WebCI and CLI interfaces. The following needs to be provisioned by the operator:

- The operator needs to configure which CSCF is capable of handling Shared IFCs. The configuration is dynamic and stored in the HssConfigDestinationHost table as an added field SupportsSharedIfc that can be turned On or Off.
- The Shared Initial Filter Criterias that will be used must be defined in the HssSharedInitialFilteringCriteria table. Each of these Shared IFCs are identified by a SharedInitialFiltCritID.
- For each Shared Initial Filter Criteria defined, Shared Service Point Triggers can also be defined in the HssSharedServicePointTrigger table. Each of these Shared SPTs are identified by a SharedServicePointTriggerID.
- A list of Shared IFCs can be assigned to a service profile by linking the identifier of the Shared IFC to that Service Profile.

Finally, the operator can configure the CSCF that will be using Shared IFCs, create the Shared IFCs and save it in the database repository, read those Shared IFCs from the database repository and modify or delete them. The operator may also link them to service profiles, as well as remove those links.

Once the proper configuration and provisioning has been done in the IMS-HSS in order to use the Shared IFCs feature and that the S-CSCF also supports this feature, subsets of Initial Filter Criteria may be shared by several service profiles. To do so, the IMS-HSS downloads the shared IFC sets implicitly by downloading the unique identifiers of the shared IFC sets to the S-CSCF. By means of a locally administered database, the S-CSCF then maps the downloaded identifiers onto the shared IFC sets. For shared IFC to be useful they have to be provisioned in the CSCF database as well.

Note: In using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and IMS-HSSs consistent. The CSCF database shall have exactly the tables shown in the figure below.

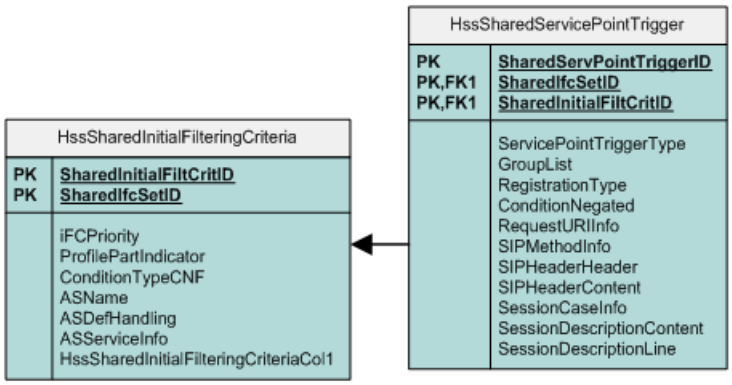


Figure 61: The CSCF's database schema for the support of Shared IFC

If the S-CSCF does not support this feature, the IMS-HSS does not download identifiers of shared IFC sets. Instead as a default behavior the IMS-HSS (by means of a locally administered database) downloads the IFCs of a shared IFC set explicitly. The IMS-HSS encodes the shared IFCs as if they were regular IFCs of the given service profile.

If the IMS-HSS does not support this feature, no special default behavior is required for the S-CSCF.

IMS-HSS Tekelec enhanced features

Administrative Registrations

The IMS-HSS must inform the S-CSCF that the served user is *administratively registered*. That means that:

- Without using the REGISTER mechanism, the user must be considered as always registered by the S-CSCF:
  - The user state and profile must be kept by the S-CSCF until the system stops or restarts;
  - Only the IFCs from the "registered" part of the user profile are processed (originating and terminating).
  - On the IMS-HSS, the user is always set to "registered" state, in order to correctly process LIR requests in terminating mode.
  - `LIA` with `ERROR_IDENTITY_NOT_REGISTERED` will never be returned for a Public Identity linked with an administrative registered Private Identity.

The S-CSCF can discover that the user is administratively registered when performing one of the following operations for the first time since S-CSCF system startup:

- First originating call request from this user;
- First terminating call request directed to this user;
- First registration from this user.

At the same time, the S-CSCF must learn the administratively registered endpoint (AREP) contact address, to use for terminating calls to this user, that otherwise would have been provided by the REGISTER mechanism.

The operator can provision this feature through the CLI and WebCI by provisioning each Hss Subscription with the following parameter:

- "AdministrativeCSCF". This parameter allows you to define the name of the CSCF linked to the IMS Subscription that will be used if the Administrative Registration feature is enabled (AdminRegistration=1).

Moreover, this feature can be enabled/disabled and provisioned through the CLI and WebCI by provisioning the following two attributes of the HssPrivateIdentity table:

- "AdminRegistration", which is the flag that can be set On/Off in order to enable/disable the Administrative Registration feature. "ContactAddress", which is useful if the Administrative Registration feature is enabled, contains the SIP URI contact address and path for terminating calls.

An administratively registered endpoint (AREP) is represented by a Private User Identity with the "administratively registered" flag set and a contact address.

As consequences:

- As any other Private Identity(PRID), an administrative registration Private User Identity (ARPRID) can be associated to zero, one or more Public User Identity implicit registration sets;
- Conversely, a Public User Identity implicit registration set may be associated to zero, one or more PRID, which can have the "administratively registered" flag set or not set.

For more information on the HssPrivateIdentity table and its new parameters, refer to the "HSS entities" section in the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision these parameters in the HssPrivateIdentity table, refer to section "Viewing/Editing HSS Subscriber Profiles" in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Support of Access Restriction

The IMS-HSS supports MAA messages containing the proprietary Access-Restriction AVP. The Access-Restriction AVP field provides restrictions on the access network and IP address used by the UE. To include this AVP in the MAA messages, the Access-Restriction must be provisioned for specific Private Identities. This can be provisioned through the CLI and WebCI by provisioning the following parameter in the HssPrivateIdentity table:

The "AccessRestriction" parameter can be provisioned on a per Private Identity basis in order to support the Access Restriction feature. This parameter allows the operator to define the list of allowed IP addresses/ranges that are restricted.

For information on the AccessRestriction parameter, refer to the HssPrivateIdentity table defined in "HSS entities" section in the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision the HssPrivateIdentity table with this parameter, refer to "Viewing/Editing HSS Subscriber Profiles" in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Support of a bad password counter

The "bad password counter" feature is handled by the IMS-HSS to monitor the number of bad password entered by a user for authentication and to eventually lock that user's private Identity in the case where the bad password counter has reached the limit.

In the case where a user provides a wrong password when registering, the authentication procedure fails and the S-CSCF finally answers to the second `REGISTER` with "`403 Forbidden`".

Additionally, it informs the IMS-HSS of the failed attempt, thanks to a **`SAR`** with:

```
Server-Assignment-Type = AUTHENTICATION_FAILURE
```

In this case, the IMS-HSS:

- Must not change the registration state of the user;
- Must increment the "bad password counter"; if it is relevant (i.e., if a counter limit has been provisioned).

Note: The SAR "AUTHENTICATION_FAILURE" is sent regardless of the current counter value and if the number of "bad password" attempts must be monitored or not.

The only purpose of this SAR is to notify the use of a bad password. So it must not be sent by the S-CSCF in other cases where the authentication fails (e.g. the access network or the UE IP address is not allowed): the behavior in those cases is to send a SAR with Server-Assignment-Type = AUTHENTICATION_TIMEOUT to the IMS-HSS.

Since the "AUTHENTICATION_FAILURE" value is used to report the use of a bad password, the use of "AUTHENTICATION_TIMEOUT" is proprietary.

The decision to lock a private ID is made on the IMS-HSS when receiving a SAR "AUTHENTICATION_FAILURE" that makes the counter reach the limit.

Each time the authentication is successful, the IMS-HSS receives a SAR with

Server-Assignment-Type = REGISTRATION or

RE_REGISTRATION. In this case and if the PRID is not locked yet, the IMS-HSS must reset the "bad password counter" to 0.

The IMS-HSS verifies if the Private Identity is not blocked during UAR/UAA exchange: the IMS-HSS answers a UAA with a reason code AUTHORIZATION_REJECTED if the Private Identity is locked (but only when PRID is provided in REGISTER).

The bad password counter is associated to a specific Private Identity and it is possible to provision it with a limit through CLI or WebCI, by provisioning the following HssPrivateIdentity table's parameter:

- The "MaxBadCounterPasswd" allows to provision a limit in order for the bad passwords to be monitored.

Refer to the "IMS-HSS entities" section in the *SDM Subscriber Provisioning - Reference Manual* for more information on this parameter. For step-by-step instructions on how to provision the HssPrivateIdentity table with this parameter, refer to the "Viewing/Editing IMS-HSS Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Moreover, the two following operations are made available in the CLI to allow the administrator of the system to unlock a Private Identity and reset to 0 the "bad password counter" in the IMS-HSS:

- **DisplayPasswdCounter**: shows current bad password counter value for a given Private Identity;
- **ResetPasswdCounter**: resets bad password counter concerning a given Private Identity and unlocks it.

Refer to section "IMS-HSS Operations" in the *SDM System Configuration - Reference Manual* for more information on how to perform these operations.

IMS-HSS Default iFCs for unregistered users

With this feature, the ORIGINATING_UNREGISTERED value has been added to the SessionCaseInfo parameter of the HssServicePointTrigger entity. This value is provided to the S-CSCF within the subscriber profile, in the "SessionCase" XML element of the SAA or PPR messages. This allows for one or several iFCs to be defined as "default" and to be downloaded to the CSCF even when the subscriber is not registered. The WebCI has also been updated to reflect the addition of this new value.

ENUM support

With this feature, an ENUM Server has been implemented as an additional functionality integrated in the IMS-HSS Service's Hss process. The HSS Service can now perform Telephone number mapping through the ENUM Server, which consists of a server that uses the ENUM (Electronic Number Mapping from E.164 Number Mapping) standard. The ENUM Server is based on the DNS protocol that is able to answer to DNS query containing NAPTR DNS Record.

The ENUM Server performs telephone number mapping to unify the telephone number system of the public switched telephone network with the Internet addressing and identification name spaces. Telephone numbers are systematically organized in the E.164 standard, while the Internet uses the Domain Name System for linking domain names to IP addresses and other resource information.

Hence, the ENUM Server is responsible for servicing a given telephone number by simple lookups in the Domain Name System. It uses special DNS record types to translate a telephone number into a Uniform Resource Identifier (URI) or IP address that can be used in Internet communications.

This allows IP-based service providers to route calls from SS7 networks (using telephone numbers in E.164 format) to either pre-IMS or IMS networks (using a SIP URI, IMS Public Identity or simply an IP address). It also allows them to route their VoIP subscribers to VoIP subscribers in other networks, using a telephone number. The ENUM Server offers a way to map telephone numbers to URIs, and therefore keep the entire communication over IP signaling (no need to route such calls through SS7 networks).

Hereunder is a description of the communication logic between the external Gateway and the Enum Server, as well as a description of the Enum Server's behavior:

- The PABX or Gateway responsible for routing a call from one network to another sends DNS Queries for Record NAPTR to the Tekelec's HSS ENUM Server. The ENUM Server is only able to accept DNS Queries for Record NAPTR. All DNS messages other than DNS Queries set with a Question for Record NAPTR are not accepted, which means that the steps described below are not executed and the Enum Server sends back a DNS Answer with DNS NOT_IMPLEMENTED.
- A DNS Query is sent in the form of a dotted Internet address, which is built from the telephone number and the domain name. For example, the fully qualified telephone number 1-315-567-1234 would turn into 4.3.2.1.7.6.5.5.1.3.1.e164.arpa. The digits are reversed because DNS reads right to left. The top level domain such as .com (or in this example: .arpa) in a URL is read first.
- The Enum Server then extracts the following from the DNS Query:
  - The telephone number, by reversing back the NAPTR Name part of the dotted internet address. (i.e.: 1-315-567-1234)
  - The domain name. (i.e.: e164.arpa)
- The Enum Server can now verify the following:
  - In the case where the DNS Query is supported and accepted, but the extracted domain name is not found in the list of supported domain names configured in the database's DNSDomainNameList entity, the Enum Server sends back a DNS Answer with DNS NXDOMAIN "non-existent domain".
  - In the case where the DNS Query is supported and accepted, but the extracted phone number doesn't exist in the database (no Enum User with such phone number have been defined), the Enum Server sends back a DNS Answer with DNS NXDOMAIN "non-existent domain".
  - In the case where the DNS Query is supported and accepted and the extracted domain name and phone number are both found in the IMS-HSS's database, the Enum Server builds a successful

DNS Answer with the information found in the database. The DNS Answer includes the following information provisioned for the Enum User in the IMS-HSS's database: Order, Preference, Flags, Services, Regular Expression (IP Addresses), Replacement, TTL.

With the information received in a successful DNS Answer, the PABX or Gateway can now route the call, using the corresponding IP address, to the IP network's destination node.

The following entities have been implemented with this feature and the operator can provision them from the CLI or WebCI:

- The DNS Config entity allows the operator to enable/disable the feature that supports the Enum Server. It also allows the operator to set the maximum number of Enum Users that can be configured under the same subscription Id and allows him to set the maximum memory size the ENUM cache functionality can use. Take note that the Enum Server functionality is disabled by default and cannot be enabled during running time of the system. The HSS Service must first be stopped before being able to change the activation status of this feature. The ENUM cache functionality is disabled by default and can be enabled dynamically by the Network Operator (without interrupting the ENUM Server) by setting, from the WebCI, the EnumCacheSize parameter with a value other than '0'.
- The DNSListenAddresses entity allows the operator to define the different DNS Listen Addresses (up to 2 listen addresses can be configured for the whole system) and Port Numbers on which the DNS Server will listen for incoming DNS Queries trough UDP transport.
- The DNSDomainNameList entity allows the operator to define the different Domain Names supported by the Enum Server.
- The DNSEnumUserTemplate entity allows the operator to define templates that can be assigned to Enum users.
- The DNSEnumUser entity allows the operator to provision ENUM users by defining each Enum User with a telephone number, domain name and the information that needs to be returned in the DNS Answer. This entity allows the Network Operator to assign a DNS ENUM Template to the user. Each Enum User is stored under a specific SubscriptionId. This allows an ENUM User to be grouped with a IMS-HSS and AAA User. One single subscriber with the SubscriptionId 'X' can have one or all of the following subscriber profiles: HLR, SIP, IMS-HSS, AAA, WiMAX, Enum.

For more details on the DNSConfig, DNSListenAddresses, DNSDomainNameList and DNSEnumUserTemplate entities and their parameters and values, refer to *ENUM Server* of the *SDM System Configuration - Reference Manual*. For instructions on how to configure the DNSConfig, DNSListenAddresses and DNSDomainNameList entities, refer to the "Enum Server" section of the *SDM System Configuration - User Guide*.

For more details on the DNSEnumUser entity and its parameters and values, refer to the "Enum Server" section of the *SDM Subscriber Provisioning - Reference Manual*. For instructions on how to provision subscribers in bulk with Enum User profiles, refer to the "Enum Server" section of the *SDM Subscriber Provisioning - User Guide*. For instructions on how to modify from the WebCI a subscriber's profile to provision it with an Enum User, refer to the "Viewing/Editing DNS ENUM Users" section of the *SDM Monitoring, Maintenance, Troubleshooting - User Guide*.

AAA Features

AAA Server functionality

The AAA Server is a RADIUS server integrated within the HSS process of the SDM system. Its core functionality is to provide Authentication and Authorization services to RADIUS enabled network access servers (NAS), such as GGSNs, Dial-up servers, BRAS, etc.

The AAA Server's core functionality is designed as per the following RFCs:

- RFC 2865
- RFC 2866
- RFC 3576
- RFC 3748 (EAP)
- RFC 3759 (EAP over Radius)
- RFC 4186 (EAP-SIM)
- RFC 4764 (EAP-PSK)
- RFC 5216 (EAP-TLS)
- RFC 5281 (EAP-TTLS)

More specifically, the AAA's functionalities are as follows:

- Handling of RADIUS authentication and authorization
- Support for the following authentication schemes: PAP, CHAP and EAP (EAP-SIM, EAP-PSK, EAP-TLS or EAP-TTLS methods). Note that the AAA supports the use of the EAP authentication algorithms for requests coming from a node other than a WiMAX node.
- Ability to dynamically allocate IP addresses from preconfigured address allocation policies. Where applicable, allocation makes use of criteria in the Access-Request message.
- Function as RADIUS Accounting proxy. The AAA Server will proxy RADIUS Accounting requests to a list of preconfigured Accounting servers. If no servers are configured, or no reply is received, the AAA Server will automatically provide an Accounting response.
- Initiate the deallocation of a previously allocated IP address, based on an administrator action.
- Function as a RADIUS Authentication Proxy. The SDM AAA Server will forward RADIUS authentication requests (Access-Request messages) to a list of preconfigured remote authentication servers based on a series of conditions. If no servers are configured or if the conditions are not met, the SDM AAA Server will perform the authentication and provide an authentication response.

The AAA Server's core functionalities can all be provisioned through the WebCI and CLI interfaces. The following needs to be provisioned by the operator:

- The AAAConfig table must be configured at system startup to activate the AAA functionality and configure it.
- The AAANetworkAccessServers table must be configured with a list of allowed NAS that are able to send Radius packets to the AAA Server. This also allows the operator to configure the secret key that is shared between the AAA server and the NAS.
- The "AuthenticationProxyModeEnable" parameter has been implemented into the "AAAConfig" entity to allow the operator to enable/disable the AAA RADIUS Authentication Proxy functionality.
- The AAANASAuthenticationServers entity allows to configure the NAS-level list of remote authentication servers to which authentication requests are forwarded. If the Authentication Proxy

Mode is enabled, this entity is accessed first when an authentication request is received. If the message comes from a NAS defined in the entity, the Called-Station-Id or the Realm is then checked, depending on the association type defined for the NAS in the entity. If the relevant Called-Station-Id or Realm matches the information associated with the NAS, the authentication request is then forwarded to the indicated remote server. If the NAS is not defined or the Called-Station-Id or Realm do not match the information in the entity, the AAASystemAuthenticationServers entity is read next.

- The AAASystemAuthenticationServers entity allows to configure the system-level list of remote authentication servers to which authentication requests are forwarded in case the NAS authentication server list is not defined or its conditions are not met. The AAASystemAuthenticationServers entity also contains Called-Station-Id or Realm associations. If the Called-Station-Id or Realm in the message matches the information in the entity, the authentication request is forwarded to the indicated remote server. If there is no match, the SDM AAA Server performs the authentication and provides an authentication response.

The AAA Server's core functionalities can all be provisioned through the WebCI and CLI interfaces. The following needs to be provisioned by the operator:

- The AAAConfig table must be configured at system startup to activate the AAA functionality and configure it.
- The AAANetworkAccessServers table must be configured with a list of allowed NAS that are able to send Radius packets to the AAA Server. This also allows the operator to configure the secret key that is shared between the AAA server and the NAS.
- The "AuthenticationProxyModeEnable" parameter has been implemented into the "AAAConfig" entity to allow the operator to enable/disable the AAA RADIUS Authentication Proxy functionality.
- The AAANASAuthenticationServers entity allows to configure the NAS-level list of remote authentication servers to which authentication requests are forwarded. If the Authentication Proxy Mode is enabled, this entity is accessed first when an authentication request is received. If the message comes from a NAS defined in the entity, the Called-Station-Id or the Realm is then checked, depending on the association type defined for the NAS in the entity. If the relevant Called-Station-Id or Realm matches the information associated with the NAS, the authentication request is then forwarded to the indicated remote server. If the NAS is not defined or the Called-Station-Id or Realm do not match the information in the entity, the AAASystemAuthenticationServers entity is read next.
- The AAASystemAuthenticationServers entity allows to configure the system-level list of remote authentication servers to which authentication requests are forwarded in case the NAS authentication server list is not defined or its conditions are not met. The AAASystemAuthenticationServers entity also contains Called-Station-Id or Realm associations. If the Called-Station-Id or Realm in the message matches the information in the entity, the authentication request is forwarded to the indicated remote server. If there is no match, the SDM AAA Server performs the authentication and provides an authentication response.
- The AAASystemAccountingServers table allows to configure the per system list of accounting applications to which accounting requests are forwarded in case the "per NAS accounting applications list" is not defined.
- The AAANASAccountingServers table allows to configure the NAS system list of accounting applications to which accounting requests are forwarded. This table is read first when an accounting request is received. If there is a NAS that matches the one from which the accounting request is coming from, the accounting application IP address is retrieved, and the accounting request is forwarded to that address.
- The AAAUserId table allows to provision AAA users and provision them with AAA User Vendor Attributes.

For more details on the AAA configuration tables and their parameters, please refer to the "*AAA"* chapter in the *SDM System Configuration - Reference Manual*. For more details on the AAAUserId table and its parameters, refer to the "AAA" chapter in the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision these tables and execute the restore operation, please refer to the "AAA Application Configuration" section of the *SDM System Configuration - User Guide*, to the "Viewing/Editing AAA Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide* and to the "AAA Operations" section in the *SDM System Configuration - Reference Manual*.

The AAA Server also has a number of extensions which provides additional flexibility to the authentication and IP allocation algorithms. One such extension is the ability to define a static IP address allocation mechanism. Refer to *Extension to handle static IP Address allocation* for more details.

3GPP Gi interface support

The AAA Server also provides support for RADIUS authentication on the 3GPP Gi interface, as specified in 3GPP TS 29.061. This includes support for 3GPP Vendor Specific Attributes (VSA) and the ability to use the 3GPP VSAs as criteria in the IP allocation process.

AAA Address Allocation

As stated above, the AAA server can be used to dynamically allocate IP addresses to users at Authentication from pre-configured address allocation policies and based on selection criteria retrieved from the RADIUS messages. The AAA™ implements an IP address allocation feature that is compliant to RFC 2865, 2866 and to 3GPP TS 29.061.

This feature can be provisioned through the WebCI and CLI interfaces. The following needs to be provisioned by the operator:

- The AAAAddressAllocationPolicy table is implemented to contain the list of all the address allocation policies. This table must be configured first. This list is always present and should have, at least, the system associated address allocation entered.
- The AAAAddressAllocationRanges table is a configurable table to specify address ranges and associated allocation policy. For a range of IP addresses to be entered it must belong to a named allocation policy that exists in the AAAAddressAllocationPolicy table. The AAA server Ranges are associated with a named allocation policy. Ranges are specified using high and low addresses. It is possible to have many range entries for an allocation policy. A field, LastAddressAllocated, is provided to keep track of the latest address allocated. This value is used as the new low value for the range.
- The AAAAddressAllocationAssociation table must be provisioned to create an association between the allocation policy and the Realm or Called-Station_id. An allocation policy may be associated with one or more Called Station Ids or one or more Realms but may not be associated with a combination of Realms and Called Station Ids. A configuration parameter is provided to specify which type of association an allocation policy has.
- The UserIPAddress table contains addresses that have been assigned to AAA users. The fields of this table are AllocationPolicyName, UserName and IPAddress. When an address that has been assigned to a user is given back the entry for that address has its UserName field set to NULL. When an address is to be provided for a user the UserIPAddress table is queried first to retrieve an address whose UserName field is NULL, if one exists. If this query returns an entry, that entry has its UserName field set to the current user. If no entries are returned by this query the next sequential address will be provided by and IP Address generation function. An entry is then made in the UserIPAddress table for this IP Address and the current user.

The IP Address generation function uses the range values specified in these tables as well as the last address generated to generate the next sequential address. When an Access-Request is received, the AAA Server performs authentication on the user, after which an Access Level is determined depending on if the authentication is successful or not. For an unsuccessful authentication, the system sets the Access Level parameter to "Unrestricted". The Access Level is used with the APN or NAI to select the appropriate address allocation to be used to provide an IP Address for the user.

For more details on these tables and their parameters, please refer to the "AAA Provisioning Configuration" section in the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision these tables and execute the restore operation, please refer to the "Configuring Address Allocation Policies and IP address pools" section in the *SDM System Configuration - User Guide* and to the "AAA Operations" section of the *SDM System Configuration - Reference Manual*.

IP Address based on Calling Station-Id Attribute

The AAA™ supports the Address allocation based on Calling-Station-Id Attribute (MSISDN in 3GPP Gi interworking) feature. This feature allows multiple User Equipments (UE) to be defined in one single AAA user profile and to have an IP address allocated to each of them. This means that there can be multiple Calling Station Ids (MSISDNs) defined with the same AAA user identifier: UserName. With this feature the Dynamic IP Address allocation can assign multiple addresses to the same username but different Calling Station Ids (MSISDN in 3GPP Gi interworking).

Hence, the table containing the AAA IP address information for a AAA user allows for multiple entries, by implementing the following new parameter:

- CallingStationID, which contains the Calling Station Identification to which the corresponding IP Address is allocated to.

For a AAA user, the AAA IP Address information (AAA IP Address, NAS IP Address and CallingStationID) can be displayed by executing the DisplayUserStatus() operation from the CLI. For more information on this operation, please refer to the "*AAA operations"* in the *SDM System Configuration - Reference Manual*.

To display this table from the WebCI, you can click on the "DisplayUserStatus" button from within a AAA user profile. For step-by-step instructions on how view this information from the WebCI, please refer to the "Viewing/Editing AAA Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Even Allocation of IP Address

This feature allows the support of an alternative method of generating an IP Address. The AAA can allocate IP Addresses by following two methods. The original method consists in looking for a free address and allocating that first IP address that becomes free. The alternative method implemented in this feature allows the AAA to support the even allocation of IP addresses. This means that it is capable of continuously re-using evenly the whole IP address range of an address pool. To achieve this, the AAA allocates the least used IP address.

The main difference between the original method and the round-robin way of generating IP Addresses is in the use of the address pool. In fact, the second method uses up the complete address pool before re-using freed addresses.

In sum, the AAA supports two different methods to generate IP Addresses and the CLI and WebCI allow the operator to select one method or the other in the AAA configuration. The operator can provision this feature by:

- Provisioning the "UseFullAddressPool" flag in the AAA Address Allocation Policy table.

For more information on this table and the "UseFullAddressPool" parameter, refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision it, refer to the "Configuring Address Allocation Policies and IP Address pools" section in the *SDM System Configuration - User Guide*.

Extension to handle Restricted Access for Unauthorized Users

The "Extension to handle Restricted Access for Unauthorized Users" feature has been implemented in order to provide IP addresses for users who don't pass authentication. To achieve this, the parameter "AccessLevel" has been implemented in the AddressPoolAssociation entity. In addition to being able to associate each address pool defined in the AddressPoolAssociation entity with one or more APNs (Called-Station-ids) or NAIs (Realms), each address pool can also be associated with an Access Level to provide IP addresses for users who don't pass authentication. An address pool that is only used for users who pass authentication can be associated with an Access Level 0 (restricted access) and an address pool that may be associated with users who don't pass authentication can be associated with an Access Level 1 (unrestricted access).

This gives the operator the flexibility to:

- Associate an address pool to one APN (Called-station-id) or NAI (Realm) which always gets used whether the user passes authentication or not, by associating it with an Access Level 1.
- Associate an APN to two different address pools, one which gets used only for authenticated users (in this case the address pool is associated with Access Level 0) and the other is used for un-authenticated users (in this case the address pool is associated with Access Level 1).
- Associate an address pool to one APN which is only to be used for authenticated users, by associating it with an Access Level 0. Un-authenticated users wanting to access this APN will receive an Access-Reject.

For more information on the "AccessLevel" parameter and its AddressPoolAssociation entity, refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision it, refer to the "AAA Provisioning Configuration - Provisioning AAA Address Allocation Policies and IP Address pools" section in the *SDM System Configuration - User Guide*.

Extension to handle static IP Address allocation

This feature provides a way for the IP Address allocation mechanism to be able to provision static IP addresses for a AAA user.

With this feature, the operator can configure a AAA user with static IP addresses for a specific Called Station (APN) or Realm. Moreover, if desired, a static IP address can also be assigned to a Calling Station (MSISDN). This allows the operator to assign an IP address per Calling Station (MSISDN) for a specific Called Station (APN).

Depending on configuration, the AAA server can provide dynamic or static IP address allocation to users. The IP addresses are selected from pre-configured IP address pools and based on selection criteria retrieved from the RADIUS message.

This brings more flexibility to the way IP Address pools can be managed.

When the AAA server receives an Access-Request message from a subscriber, for a specific Called Station (APN) or realm, the AAA server verifies if this subscriber has a static IP address assigned for that Called Station or realm. If it does, the AAA server returns the static IP address in the Access-Accept message and if it doesn't have a static IP address assigned, it dynamically allocates the IP address and returns it in the Access-Accept message.

Through the CLI or WebCI, the operator can provision this feature as follows:

- A static IP Address can be assigned to a specific Called Station (APN) or Realm and, if needed, for a specific Calling Station (MSISDN) by executing the "AssignIPAddress ()" operation. When executing this operation for a subscriber, the Called Station must be specified; the realm, on the other hand, doesn't need to be entered, it is extracted from the AAAUserName. With this information, the AAA server associates an IP Address to the Called Station or Realm from the configured IP Address pools. This IP Address is said to be static and becomes unavailable when the AAA server performs a dynamic allocation of an IP address. For a single subscriber, a different static IP Address can be assigned for each Called Station (APN) or Realm. Moreover, for a subscriber's specific Calling Station (MSISDN), different static IP addresses can be assigned for different Called Stations (APNs).
- The static IP Addresses that the AAA server has already assigned to a subscriber can be displayed by executing the "DisplayAssignedIPAddresses ()".
- A static IP Address can be released by executing the "ReleaseIPAddress ()" operation. When executing this operation for a Called Station or realm (and optionally Calling Station) of a subscriber, the AAA server releases the static IP Address that was assigned for that subscriber's Called Station or realm (and Calling Station). This means that this IP Address is now available in the pool for dynamic IP allocation and is no longer reserved uniquely for that subscriber's Called Station or realm (and Calling Station).

For more information on the operations implemented with this feature, refer to the "*AAA Operations"* section in the *SDM System Configuration - Reference Manual*.

Extended IP Address Pool Selection: IP Address allocation based on SGSN Address Attribute

This feature has been implemented to add to the AAA, the ability to select an address pool based on the combined values of SGSN Address (3GPP vendor specific attribute) and Called Station Id, or on just the SGSN Address.

With this feature, the AAA behaves as follows:

- In the case where the AAA doesn't receive the SGSN Address attribute in the Access-Request message:
  - The AAA proceeds with the pool selection using one of the following attributes: NAS ID, Called Station Id or Realm.
- In the case where the AAA receives the SGSN Address attribute in addition to the Called Station Id in the Access-Request message:
  - If in the database there is an address pool associated with both the received SGSN Address and Called Station Id combined:
    - The AAA uses that pool that is associated with both of the received SGSN and Called Station Id combined to allocate an IP address.
  - If in the database there is an address pool associated only with the received SGSN:
    - The AAA uses the pool associated with that received SGSN to allocate an IP address.
  - If in the database there is no address pool associated with the received SGSN:

- The AAA tries to retrieve an address pool associated with the received SGSN, but when no success, the AAA proceeds with the pool selection by using one of the following attributes: NAS ID, Called Station Id or Realm.

Finally, the order of priority for pool selection is the following:

1. SGSN Address combined with Called Station Id
2. SGSN Address
3. NAS ID, Called Station Id, Realm.

With the implementation of this feature, the following has been added to the AAAAddressAllocationAssociation entity in order to allow the operator to associate an address pool to a SGSN Address or to a combined SGSN Address/Called Station Id:

- The AuxiliaryValue attribute allows the operator to define, for a specific pool, the Called Station Id in the case where the association type is the SGSN Address combined with the Called Station Id.
- The following values have been added for the AssociationType attribute:
  - SGSN_CalledStationId
  - SGSNAddr

Refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual* for more details on the AAAAddressAllocationAssociation entity and its attributes and values. For instructions on how to provision address pools and on how to associate them to the different selection attributes (SGSN, SGSN/CalledStationId, NAS ID, Called Station Id, Realm), refer to the "Configuring Address Allocation Policies and IP Address Pools" section of the *SDM System Configuration - User Guide*.

Optional allocation of IP address

This feature gives the operator the option to be able to turn off the AAA's IP address allocation functionality. With this feature, the operator can chose to provision the AAA to perform authentication for a user without providing a user IP address.

In order to implement this IP address allocation policy, the AAAAddressAllocationPolicy entity has been updated as follows:

The AllocationPolicyType attribute has been added with the following possible values:

- AddressPool: Setting this attribute to this value means that the AAA can proceed with the IP Address allocation as already implemented.
- NoIP: Setting this attribute to this value means that the AAA doesn't need to proceed with the IP address allocation procedure and instead returns an Access-Accept without an IP Address following a successful authentication.

When receiving an Access-Request for a user, the AAA uses the previously implemented selection scheme based on SGSN+APN, SGSN, NAS, APN or Realm for IP address pool selection. Once the IP address pool is selected, it then proceeds or not with the IP Address allocation procedure depending on the policy type provisioned for the pool selected in the AAAAddressAllocationPolicy entity.

Refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual* for more details on the AAAAddressAllocationPolicy entity and its attributes and values. For

instructions on how to provision an address pool, refer to the "Configuring Address Allocation Policies and IP Address Pools" section of the *SDM System Configuration - User Guide*.

Operation to clear an IP address pool

This feature gives the operator the option to be able to manually reset (de-allocate) some or all the IP addresses within a specific address pool that have been allocated to subscribers.

To achieve this, the 'ClearAddresses' operation has been implemented and can be executed by the operator from WebCI, CLI or through XML requests. This operation is available for each address pool entry in the AAAAddressAllocationPolicy entity.

This operation can be executed for one single IP Address pool at a time. Since this operation allows to free up IP Addresses based on how long ago they were allocated to subscribers, the following parameter must be specified when executing this operation:

- OlderThan: age in seconds.

This allows to free up IP addresses, within a specific address pool, that have been allocated to subscribers for the longest time.

The operation will clear all IP addresses within the defined pool that are older than the specific age. Setting "age" to 0 will clear all IP addresses.

Refer to the "AAA Operations" section of the *SDM System Configuration - Reference Manual* for instructions on how to execute the ClearAddresses operation from the CLI and refer to the "Configuring Address Allocation Policies and IP Address Pools" section in the *SDM System Configuration - User Guide* for instructions on how to execute this operation from the WebCI.

Logging of IP Address allocation

The Logging of IP address allocation feature generates logs for the allocation and de-allocation of IP addresses done by the AAA, for selected address pools.

These logs are written into audit files which can be found on each of the System Controller blades (active and standby) under the following directory: /export/audit.

Each log message consists of the following pieces of information:

- Timestamp: the time at which the allocation/deallocation was performed
- Pool Name: the address allocation policy name associated with the IP address
- MSISDN: the MSISDN to which the IP address is assigned
- IP Address: the address which was allocated or deallocated
- Event: a two-letter code describing the action which was performed. Hereunder is the list of event codes that can be generated. Note that there are several OAMP operations that may cause the de-allocation of an IP address as a side-effect:these are enumerated as D1, D2,D3,D4 and D5.

EVENT CODE	EVENT DESCRIPTION
AD	Allocation of a dynamic IP address as a result of an access-request message.
AS	Allocation of a static IP address as a result of an access-request message.
DS	Deallocation of an IP address as a result of an accounting-request (stop) message.
DT	Deallocation of an IP address by the AAA due to a timeout.

D1	Deallocation of an IP address as a result of a ClearAddresses operation.
D2	Deallocation of an IP address as a result of the deletion of an Address Pool Range.
D3	Deallocation of an IP address as a result of the update of an Address Pool Range.
D4	Deallocation of an IP address as a result of a DisconnectNAS operation.
D5	Deallocation of an IP address as a result of a DisconnectUser operation.

The audit files are classified into two categories:

- The current audit file. Format: <Audit Component>.<Extension>
- The previous audit file. Format: <Audit Component>-<Timestamp>.<Extension>
- The Audit Component represents the information which is audited, ex: AaaIp. The timestamp represents the time when the audit file is created and has the format yyyymmddhhmmss. The file extension represents the audit data format, which can be: csv (comma-separated values) or xml (Extensible Markup Language).

The audit files are also rotated when the following triggers are met:

- The daily time has reached midnight.
- The audit file contains more than 100 000 lines.

The old audit file cleanup will be done on a daily basis at midnight based on the configurable number of history days set by the Network Operator through a SDM Interface. In the case of multiple audits, the cleanup is done per audit component.

The following has been implemented in the database in order to allow the Network Operator to manage the audit files (prior to starting them) through the SDM Interfaces:

- The new AuditManager entity has been implemented to allow the Network Operator to configure:
  - The Audit log message format (CSV or XML)
  - The number of days that the old audit log files must be kept in the /export/audit directory.
  - The debug information request in order to request the following debug information to be included in each audit line: slot, module, file and line. By default, this debug information is not included.
- The new AuditInfo entity has been implemented to allow the Network Operator to view the information that is being audited (only the AaaIp is supported for now) and its audit status: Enable or Disable.
- The newly implemented StartAudit() and StopAudit() operations allow the Network Operator to start/stop an audit component dynamically (with no system restart). When an audit component is started, a new current audit file is created under /export/audit (on both SC). And when an audit component is stopped, the current audit file will be renamed to old audit file, so that the external tools can connect and get all the audit files during audit period. The operator must be careful when activating the audit logging feature because the performance impact will be on the blades where applications are running and also on both SCs.

In addition to being able to turn on or off the generation of audit files on a global level, the AuditLoggingEnabled flag has been implemented in the AAAAddressAllocationPolicy entity in order to allow the Network Operator to enable/disable this feature on a per-pool basis. In other words, this flag determines whether or not the logs will be generated for the IP addresses associated with the pool.

For a detailed description of the AuditManager and AuditInfo entities and their attributes as well as for a description of the StartAudit() and StopAudit() operations, refer to the "Audit log file Management" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. For more details on how to configure and enable/disable the audit loggings per audit component, refer to the "Configuring and Enabling/Disabling Audit loggings" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

PDP Disconnection initiated by the RADIUS Server

As mentioned previously among the core functionalities of the AAA Server, Disconnect-Request packets can be sent by the AAA, as per the RFC 3576, in order to terminate a user session on a NAS and discard all associated session context. With such a feature, the operator can initiate the deallocation of a previously allocated IP address. Through the CLI or WebCI, the operator can disconnect a user that was authenticated and had an IP address assigned to it with the following operation:

- DisconnectUser which is available on a per subscriber basis.

Refer to the "AAA Operations" section of the *SDM System Configuration - Reference Manual* for more details on this operation.

RADIUS 3GPP Vendor Specific Attributes

The AAA™ implements a Vendor Specific Attributes feature that is compliant to RFC 2865, 2866 and to 3GPP TS 29.061.

The AAA Server is equipped to support and interpret the vendor-specific information sent by a client. This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage.

With such a feature, the operator can provision the vendor specific attributes on a per user basis. Through the CLI or WebCI, the operator can add, modify, delete and display User Vendor Specific Attributes in the new AAA UserVendorAttribute table. For more information on this table and its parameters, refer to the "AAA" chapter of the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision it, refer to the "Viewing/Editing AAA Subscriber Profiles" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

RADIUS server query to correlate IP addresses and Calling Station IDs (MSISDN)

This feature has been implemented to provide the AAA server with the capability to give application servers with additional user information. This enables operators to offer value added services by allowing the users faster access to applications by providing the Calling-Station-Id (MSISDN) as a mean of identification based on the IP address.

When the AAA server receives an Access-Request with an IP address for a user configured as a "special user", it sends back a proprietary Access-Accept response, which includes the Calling-Station-ID (MSISDN) of the user.

For the AAA server to be able to achieve this, the operator must provision the following through the CLI or WebCI:

The operator must define the AAA Users for which he wishes the AAA server to send the MSISDN in the Access-Accept response to the Access-Request. For this, the operator must configure the "SpecialUser" parameter in the AAAUserId entity. For AAAUserIds configured as being a "special

user", the AAA server sends, in the Access-Accept message, the Calling-Station-Id (MSISDN) of the user, based on the IP Address provided in the Access-Request.

The operator must also define the different IP Address Pools allowed for each AAA "special user". To do so, the operator must provision the AAAUserIPAddressPools entity. Each "special user" can be configured with one or more IP Pools to query. If no IP addresses are specified in a pool, it is called a blank pool and in this case, all the pools can be queried.

Once the AAA server receives an Access-Request for a AAA user configured as a "special user", the AAA server verifies if the IP Address supplied with the request is in-use. If so, the AAA server bases itself on that IP Address to obtain the IP Address Pool name, with which the AAA server finds the AAAUserName from the AAAUserIPAddressPools entity. Then, with the AAAUserName, the AAA server can locate the Calling-Station-Id in the database and finally retrieve it in order to insert it in the Access-Accept message.

For more information on the "SpecialUser" parameter and its AAAUserId entity, refer to the "AAA" chapter of the *SDM Subscriber Provisioning - Reference Manual*. For more information on the AAAUserIPAddressPools entity, refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision the SpecialUser parameter, refer to the "Viewing/Editing AAA Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*. For instructions on how to provision the AAAUserIPAddressPools entity, refer to the "Configuring Address Allocation Policies and IP Address Pools" section of the *SDM System Configuration - User Guide*.

IMS-HSS/AAA Support for Early IMS Security

With this feature, the IMS-HSS/AAA supports the security mechanisms for early IMS implementations, as per the TR33.978 standard. This allows the IMS-HSS/AAA servers to support networks that are not fully compliant with the IMS security solution specified in TS 33.203.

With the implementation of this feature, the IMS-HSS/AAA servers have been enhanced with new capabilities in order to behave as follows:

Upon receiving, from an Early-IMS Configured APN, a RADIUS Accounting Request START message that contains the IP address, the CalledStationId and one of the following attributes: User Name, IMSI (3GPP attribute), CallingStationId, the AAA tries to match the received CalledStationId with one configured in the newly implemented AaaAPNConfig table. If a match is found and the Early IMS Security feature is turned ON for this CalledStationId, the AAA/IMS-HSS treat this message as configured in the AaaAPNConfig table, using the behavior implemented for the Early IMS Security feature.

The IMS-HSS then tries to find a match between an IMPI provisioned with the Early IMS Security and one of the following attributes received in the message: the Calling-Station-Id or the 3GGP IMSI Attribute or the User Name. It is the configured information in the AaaAPNConfig table that will indicate to the IMS-HSS which attribute it must try to match with an IMPI. The match is done following the next statement:

- CallingStationId = 22222 will match 22222@domain, but will not match 922222@domain or 222229@domain.
- Imsi = 33333 will match 33333@domain, but will not match 933333@domain or 333339@domain.

Once an exact match has been found with an IMPI that is provisioned as Early IMS Security, the IMS-HSS stores the Framed IP address (IP address that has been assigned to the subscriber at registration) in the subscriber's volatile data.

If the operation was successful, an Accounting-Response is sent back to the GGSN.

This allows the S-CSCF to be able to perform the early IMS security mechanism when receiving a SIP registration request or any subsequent requests for a given IMPI, by checking that the IP address in the SIP header matches the IP address that was stored against that subscriber's IMPI in the IMS-HSS.

At the reception of a RADIUS Accounting Request STOP message for a subscriber for which the Early IMS Security has been applied, the IMS-HSS simply removes the previously registered IP address (FramedIp) from the corresponding IMPI.

To achieve this, the operator must provision the following parameters in the PrivateIdentity table (when provisioning an IMPI):

- The EarlyIMSSecurity value has been added to the AlgoName parameter when provisioning an IMPI. For an IMPI provisioned with Early IMS Security, the operator can not only set the AlgoName parameter to the new EarlylIMSSecurity value, but also to the HTTP Digest value. The IMS-HSS supports early IMS security mechanism that protects HTTP traffic in order to provide user access to various operator customized services.
- The new EarlyIMSSecurity parameter has also been added to allow the operator to define an IMPI as Early IMS Security.

Moreover, the operator needs to configure the following new table:

- The AaaAPNConfig table allows the operator to configure the following for a Called Station ID:
  - Set the Early IMS Security feature ON/OFF.
  - Select the action the AAA must take in case of Early IMS Security failure.
  - Set the attribute (CallingStationId, IMSI, User Name) for which the IMS-HSS must find an IMPI that matches.

The WebCI has been updated to allow the operator to configure this new feature and also allows to view, from a subscriber profile's Registration status table, the FramedIp stored in the IMS-HSS's database after a successful Early IMS Security procedure.

For more information on the AlgoName and EarlyIMSSecurity parameters, refer to the IMS-HSS Private Identity in the "IMS-HSS entities" section in the *SDM Subscriber Provisioning - Reference Manual*. For step-by-step instructions on how to provision a IMS-HSS Private Identity with Early IMS Security, refer to the *Adding a Private Identity to an existing Hss Subscription* procedure in the "Viewing/Editing IMS-HSS Subscriber Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

For more information on the AAA APN Configuration table, refer to the "AAA Provisioning Configuration" section in the *SDM System Configuration - Reference Manual*. For step-by-step instructions on how to provision the AAA APN Configuration table, refer to the "IMS-HSS/AAA Support for Early IMS Security Configuration" section in the *SDM System Configuration - User Guide*.

WiMAX AAA server

The AAA can now support the WiMAX access technology.

The following new functionalities have been added to the AAA in order to support WiMAX:

- WiMAX Home AAA (H-AAA) functionality
- Process RADIUS Access-Request message received from ASN-GW. The ASN-GW - AAA interface supports information transfer for authentication between the ASN-GW and the AAA.
- Process RADIUS Access-Request messages received from Home Agent. The Home Agent - AAA interface supports information transfer between the Home Agent and the AAA.

- Authenticate WiMAX users using the EAP-SIM, EAP-PSK, EAP-TLS or EAP-TTLS methods or a EAP-PASS trough method that allow Wimax Testing.
- Support of RFC 4186, RFC 4764, RFC 3579 and RFC 5281 for EAP framework
- Support multiple EAP authentication methods as well as a preferred authentication method per AAA WiMAXuser.
- Generate WiMAX Keys based on MIP-RK, HA-RK, HA-SPI, etc
- Allocate Home Agent IP addresses dynamically on a per Weight basis (round Robin, Master backup, etc.). HA allocated IP address will be in the same network than the dynamic IP address allocated for the Mobile IP.
- Automatic re-calculation of Home Agent RK upon LifeTime expiration
- Accounting Proxy: Forwarding of RADIUS accounting Requests.
- Authentication Proxy: Forwarding of RADIUS authentication requests.
- Support WiMAX profiles to be provisioned for AAA users.
- Converged AAA/IMS-HSS /HLR profiles for one single user. A same user can have a WiMAX profile, a basic AAA profile, a IMS profile and an HLR profile.
- Support several Packet Flow Descriptors per AAA WiMAX users.
- Dynamic IP allocation of the MIP with the operator Network based on per NAS-Identifier or Realm or Called_Station_ID.
- Static IP allocation for a Non Roaming WiMAX User.
- Support several WiMAX QOS Descriptors per Packet Flow Descriptor.
- Compliant to WiMAX Release 1.2.2 stage 3.
- Support of PMIP/CMIP MIP routing Key Derivation.

The AAA's role when receiving an Access-Request for a AAA WiMAX user consists in authenticating the user using either the EAP-SIM, EAP-PSK, EAP-TLS or EAP-TTLS methods. Then, the AAA generates WiMAX keys and allocates dynamically the IP address of the Home Agent (HA) the ASN-GW needs to communicate with, and sends it back in the Access-Accept message, along with the user's QoS information. For each authenticated AAA WiMAX user, the AAA creates a MIP session with all the user's specific information: Wimax Keys, IP address of the MS, CallingStationId, ASN-GW address, etc. This MIP session is used at Re-authentication time in order to return always the same Home Agent (if no ASN-GW handover detected) and the same IP address. It keeps also a context between an ASN-GW and a Home Agent for a specific user for which WiMAX Keys have been computed.

With the implementation of these new functionalities for the AAA, the WebCI and CLI have been updated to allow the operator to configure the following:

- General EAP authentication, which can be configured through the "EAPSystemConfig" entity
- The EAP-SIM authentication method, which can be configured through the "EAPSIMSystemConfig" entity.
- The EAP-PSK authentication method, which can be configured through the "EAPPSKSystemConfig" entity.
- The EAP-TLS and EAP-TTLS authentication methods, which can be configured through the "EAPTLSSystemConfig" entity.
- WiMAX capabilities, which can be configured through the "WimaxCapabilities" entity.
- WiMAX Home Agents, which can be configured through the "WimaxHomeAgent" entity.
- WiMAX QoS Descriptor, which can be configured through the "WimaxQOSDescriptor" entity.
- WIMAX packet Flow Descriptor for a Specific User that are linked with Specific QOS Descriptor can be configured on a per User basis in AAAUserId entity

The operator can provision AAA WiMAX profiles through the WebCI or SOAP interfaces. The following new parameters have been added to the "AAAUserId" entity to allow the operator to define WiMAX profiles:

- EAPSIMsimId, EAPIdentity, PreferredAuthMehtod, AuthMethod, MIPType.

For more details on these tables and their parameters, please refer to the "*AAA*" chapter in the

SDM System Configuration - Reference Manual. For step-by-step instructions on how to provision these tables and execute the restore operation, please refer to the "Configuring EAP" section of the *SDM System Configuration - User Guide*.

Authentication EAP-TLS

With this feature, the AAA server supports the EAP-TLS authentication algorithm. The EAP-TLS authentication algorithm is based on the X.509 chain of trust mechanism. To achieve this, the AAA server now allows for Root Certificates (Authorities) and Server Certificates to be stored in its database. This information among other EAP-TLS configuration parameters must be defined at configuration of the AAA server. The WebCI displays this information within the following tables, which are accessible from the **AAA** folder, in the EAP-TLS tab of the EAP Configuration window:

- The EAP-TLS table allows to view and modify some configuration parameters that are stored in the EAPTLSSystemConfig entity.
- The Server Certificates table allows to view and provision the Server Certificate (stored in the X509ServerCertificates entity), which is sent by the AAA server to identify itself to the subscriber device for EAP-TLS authentication.
- The Root Certificates table allows to view and provision Root Certificates (stored in the X509RootCertificates entity) used by the AAA server to validate the subscriber.

Moreover, the following operation has been implemented and can be executed from the WebCI:

- The LoadPEMFile() operation allows the operator to load into the SDM's database, the X.509 Certificate files received.

The AAA server also allows for this authentication method to be used on a per subscriber basis. The WebCI offers the possibility to provision a AAA user with or without this authentication method. When provisioning a AAA user, the operator can now set the AuthMethod attribute to TYPE_EAP_TLS.

In the case where the AAA server is configured with the EAP-TLS and where it receives a RADIUS Access-Request from a user provisioned with the EAP-TLS authentication method, the AAA server behaves as follows:

- It exchanges proper certificates with the subscriber's device by sending its Server Certificate through a RADIUS Access-Challenge message in order to allow the subscriber's device to verify the identity of the AAA server.
- It then verifies the identity of the subscriber using the Client certificate sent by the subscriber's device. The Client Certificate refers to a Root Authority Certificate which in turn is used by the AAA server to compare with the Root Certificates stored in its database:

If a match of the Root Certificate is found, the AAA server then uses this Root Certificate's cryptographic data to validate the Client Certificate's digital signature. If this validation is successful, the authentication passes and the AAA Server sends back a RADIUS Access-Accept message.

If the Root Certificate is not found, the authentication fails and the AAA Server sends back a RADIUS Deny message.

For authentication of the subscriber's device (EAP Client authentication), the operator can configure the AAA Server (EAP Server) to request or not certificates from the subscriber's device (EAP Client). To allows this, the AuthenticationClientTLS parameter has been implemented in the EAPTLSSystemConfig entity (EAP-TLS table in the WebCI).

For more information on the EAP-TLS entities and their parameters, refer to the EAP Configuration section of the *SDM System Configuration - Reference Manual*. For instructions on how to provision the AAA with EAP-TLS, refer to the Provisioning EAP Configuration section of the *SDM System Configuration - User Guide*.

Authentication EAP-TTLS

The EAP-TTLS provides a secure tunnel over which the following authentication protocols may exchange messages: PAP, CHAP and MS-CHAP-V2.

TTLS consists of 2 phases:

- The TLS handshake phase which sets up the secure channel using the EAP-TLS method and the certificates.
- The application phase during which authentication data is exchanged using either PAP, CHAP or MS-CHAP-V2 protocols. The AAA server determines which method is used for the second level authentication (PAP, CHAP, MS-CHAP-V2) based on the attributes it receives:

  User Password, ChapPassword or MS Chap Challenge.

The authentication messages are exchanged over the secure channel as encrypted RADIUS attributes. Normally, with EAP-TTLS, the EAP Server sends certificates to the EAP Client for the EAP Client to be able to authenticate the Server and the EAP Server authenticates the EAP Client once the secure tunnel is established, without requesting any Client certificates.

However, whether or not the EAP Server requests certificate(s) from the EAP Client, for client authentication, is configurable by setting the AuthenticateClientTTLS parameter to On/Off in the EAPTLSSystemConfig entity (EAP-TLS table in the WebCI). Refer to the *SDM System Configuration - Reference Manual* for more details on this parameter and its possible values.

The AAA server also allows for this authentication method to be used on a per subscriber basis. The WebCI offers the possibility to provision a AAA user with or without this authentication method. When provisioning a AAA user, the operator can now set the AuthMethod attribute to TYPE_EAP_TTLS.

AAA state/context sharing across blades

This feature allows the state/context information of WiMAX users (their WiMAX Sessions) to be shared across multiple blades by different AAA services. To achieve this, the AAA has been enhanced to store all WiMAX Sessions in the system's database. This ensures that no WiMAX sessions are lost when a AAA service fails and if the NAS sends Radius messages in a round robin manner to the system's different AAA services, it allows a AAA service to have access to any WiMAX Session information even if it didn't originally create it.

The AAA has been enhanced to:

- Manage Session timeouts in the system's database. For this, a Session Timer Manager has been implemented to compare the expiry date of each WiMAX Session with the actual date and reset the allocated IP address of expired Sessions. For this, the following parameters has been implemented and can be set and edited by the operator from the WebCI's AAA Configuration table:

- The AAA Configuration's SessionWatchdogPeriod parameter indicates the periodical value (in seconds) used to trigger the Session Timer Manager to compare the expiry date of each Session with the actual date, based on the Session lifetime defined in the AAA User Id table's SessionTimeout parameter. In the case where the Session has expired, the Session Timer Manager releases the allocated IP address by deleting the Session. By default, this parameter is set to 0, which means that the Session Timer Manager is never triggered and that the Sessions are never expired no matter what their lifetime is. This parameter can be set by the operator depending on the average Session timeout configured per user.

For more information on the new AAA Configuration's SessionWatchdogPeriod parameter, refer to the "AAA Configuration" section of the *SDM System Configuration - Reference Manual*.

For instructions on how to view and modify the SessionWatchdogPeriod parameter, refer to the "Configuring the AAA" section in the *SDM System Configuration - User Guide*.

IP Address Timeout

With this feature, an internal mechanism has been implemented in order to free IP addresses allocated to AAA users, whom may or may not be provisioned into the AAA. To achieve this, the following has been enhanced and implemented:

- The AAA server records the time stamp at each IP address allocation action.
- The SessionTimeout parameter, initially implemented for WiMAX users has been enhanced to also apply for AAA users provisioned in the AAA. It indicates the lifetime (in seconds) of the session created for a specific AAA user. It can be defined for each AAA user provisioned in the AAA, by configuring the SessionTimeout parameter in the AAA User Id table.
- The Session Timer Manager implemented for the AAA state/context sharing across blades feature has been enhanced to not only be able to manage WiMAX Sessions, but also AAA Sessions. The Session Timer Manager now compares the expiry date of AAA Sessions (using the time stamp recorded when the IP address was allocated and the lifetime of the AAA session configured for the SessionTimeout parameter) with the current date. In the case where the Session Timer Manager notices that the session has expired, it releases the allocated IP address back into the IP address pool for reallocation. The SessionWatchdogPeriod parameter (also previously implemented for the AAA state/context sharing across blades feature) can be configured from the WebCI's AAA Configuration table and triggers the Session Timer Manager to perform this operation.
- In order to allow the Session Timer Manager to also release the allocated IP address of a session created for AAA users that are not provisioned in the AAA, the following new parameter has been implemented and can be set and edited from the WebCI's AAA Configuration table:

  - The DefaultSessionTimeout parameter indicates the lifetime (in seconds) of the Sessions created for AAA users that are not provisioned in the AAA. During this lifetime, these Sessions remain valid. After the Session Timer Manager notices that this lifetime has expired, the Session is deleted and the IP address allocated to the user is reset. By default, this parameter is set to 0, which means that Sessions have an infinite lifetime and never expire.

Finally, for a subscriber provisioned or not provisioned into the AAA and for which the RADIUS session is inactive (no Accounting-Request with Acct-Status-Type=update or Acct-Status-Type=stop messages were sent from GGSN) during the period of time defined in the SessionTimeout or DefaultSessionTimeout parameter, the AAA releases the IP address reserved for that session.

WiMAX AAA DHCP Interface

The AAA supports the DHCP interface. With the implementation of this feature, it is possible to configure the AAA with DHCP data in order to allow the AAA to send Access-Accept messages for a WiMAX user that each contain DHCP data instead of an allocated IP address.

The decision to respond with an Access-Accept message containing DHCP attributes, instead of allocating an IP address, is based on the address allocation policy type provisioned for the Address allocation policy selected by the Access-Request parameters. To identify the address pool the AAA must refer to in its database in order to know what must be returned in the Access-Accept message (IP address or no IP address or DHCP data), the AAA follows the same logic as the one described in *Optional allocation of IP address* with the addition of the DHCP Identifier as another allocation policy type. When the selected address pool's allocation policy type is set to the DHCP Identifier, the AAA responds to an Access-Request message with an Access-Accept message containing DHCP attributes.

The DHCP data included in the Access-Request and Access-Accept messages are sent as the RADIUS WiMAX vendor specific attributes: WiMAX-DHCPv4-Server, WiMAX-DHCP-RK, WiMAX-DHCP-RK-Key-Id, WiMAX-DHCP-RK-Lifetime.

Note: The DHCP-RK the AAA sends in the Access-Accept is encrypted.

- The Authenticator DHCP Relay/DHCP Server sending the Access-Request are configured in the AAA and thus recognized by the AAA.
- The WiMAX user, for which the Access-Request is sent, is provisioned in the AAA and has passed authentication.
- The Access-Request contains valid WIMAX vendor specific DHCP attributes.
- The allocation policy type of the selected Address allocation policy is set to '`DHCP_ADDR`'.

More precisely, for an Access-Request coming from a WiMAX user, the AAA replies with an Access-Accept that includes a DHCP server address, an associated DHCP-RK (encrypted) and the DHCP RK key Id.

After the AAA has successfully completed authentication of the WiMAX user, the DHCP Server requests the DHCP-RK from the AAA by sending it an Access-Request with the DHCP-RK key Id given out by the AAA during authentication. To this Access-Request, the AAA responds with one of the following:

If the DHCP-RK-Key-Id received has DHCP-RK data associated to it in the AAA's database, then the AAA responds by sending back an Access-Accept with the DHCP-RK information (RADIUS Message Authenticator, WiMAX-DHCP-RK, WiMAX-DHCP-RK-Key-Id, WiMAX-DHCP-RK-Lifetime) that is associated to the DHCP-RK key Id received. The AAA server generates a DHCP-RK for each configured DHCP.

If the DHCP-RK-Key-Id received has no DHCP-RK data associated to it in the AAA's database, then the AAA responds by sending back an Access-Reject.

If the Access-Request doesn't include a Message Authenticator or if the latter fails verification, then the AAA silently discards the Access-Request message.

In order to achieve this, the following updates have been made in the AAA's database:

- The AAAAddressAllocationPolicy entity has been updated with the following:
  - The new `DHCP_IDENT` value for the AllocationPolicyType attribute, which means that the allocation policy is to return the DHCP data in the Access-Accept message.

- The new DHCPIdent attribute, which allows the operator to provision, for an Address allocation policy, the DHCP Identifier that represents the DHCP data that must be returned in the Access-Accept message.

The WimaxDHCPData entity allows to associate the DHCPIdent, from the AAAAddressAllocationPolicy entity, with a DHCP server address. With this entity, the operator can configure, for each DHCP Identifier, the DHCP data that must be returned in the Access-Accept (the IP Address of the DHCP server and the lifetime of the DHCP-RK).

Moreover, the WimaxDHCP_RK table has been added in the WebCI to allow the Network Operator to view the different DHCP-RK keys generated by the AAA.

Refer to the "AAA Provisioning Configuration" section of the *SDM System Configuration - Reference Manual* for more details on the AAAAddressAllocationPolicy entity and its attributes (AllocationPolicyType) and values.

Refer to the "WiMAX Configuration" section of the *SDM System Configuration - Reference Manual* for more details on the WimaxDHCPData and WimaxDHCP_RK entities and their parameters.

For instructions on how to set the AllocationPolicyType attribute to DHCP_IDENT for a specific Allocation Policy, refer to the "Configuring Address Allocation Policies and IP Address Pools" section of the *SDM System Configuration - User Guide*.

For instructions on how to provision the DHCP data (IP address of the DHCP server and the DHCP-RK lifetime) for each DHCP Identifier (DHCPIdentifier), refer to the "Configuring WiMAX" section of the *SDM System Configuration - User Guide*.

LTE-HSS functionality

The LTE-HSS Server is a Diameter server integrated within the Tekelec ngHLR product of the SDM system. Its core functionality is to support subscribers using the Evolved Packet Core (EPC) (also known as the System Architecture Evolution (SAE)) network architecture of the 3GPP's LTE wireless communication standard. The LTE-HSS serves as a central database that contains details of each mobile phone subscriber that is authorized to use the EPC network.

More specifically, the LTE-HSS's functionalities are as follows:

- Manage the mobility of subscribers by means of updating their position in administrative areas handled by MMEs/SGSNs. The action of a user of moving from one MME/SGSN to another is followed by the HSS with a Location update procedure.
- Send the subscriber data profile to a MME or SGSN when a subscriber first roams there.
- Remove subscriber data from the previous MME/SGSN when a subscriber has roamed away from it.
- Calculate Authentication Vectors based on the SIM credentials and sent them to MME/SGSN for validation against the ones received from the phone.
- Communicate with the SDM ngHLR's HLR-Proxy functionality in order to forward messages to an external legacy HLR, as necessary in either one of the following scenarios:
  - When the subscriber with the following characteristics is roaming between the 3G-LTE networks and vice-versa:
    - the subscriber has a 3G HLR profile provisioned in an external legacy HLR

  - the subscriber has a 4G (LTE) profile provisioned in the SDM LTE-HSS.
  - the subscriber's 'HlrProxyMode' flag is set to 'true'.
- When the subscriber's authentication credentials are provisioned in an external legacy HLR.
- Communicate with the SDM's integrated ngHLR in order to support bidirectional roaming between the 3G and LTE networks. For a subscriber with a 3G profile and a LTE profile both provisioned in the SDM system (in the Tekelec ngHLR and LTE-HSS respectively), the LTE-HSS is capable of supporting it when roaming between the 3G and LTE networks and vice versa, by communicating with the SDM's ngHLR. The subscriber's data is exchanged between the Tekelec ngHLR and the LTE-HSS internally and is transparent to any external node (MME/SGSN).

The SDM system's LTE-HSS is 3GPP Release 9 (TS 29.272 v9.0.0) compliant and has been fully integrated with the GSM/UMTS ngHLR, which means that it shares the following with the Tekelec ngHLR:

- subscriber profile
- volatile data
- AuC
- SW/HW platform
- provisioning stream

The LTE-HSS is connected to an MME or a SGSN using the Diameter Protocol defined by the IETF in the RFC3588. The under layer transport that is used to connect two diameter peers (LTE-HSS and MME for instance) is TCP or SCTP. The Diameter interface used between the LTE-HSS and the MME is named S6a while S6d is the one used between the LTE-HSS and the SGSN.

Through these interfaces, the LTE-HSS supports the following types of messages for Location Management procedures:

- Update Location Request/Answer (ULR/ULA), Cancel Location Request/Answer (CLR/CLA), Purge UE Request/Answer (PUR/PUA) messages for Location Management procedures.

  The Update Location Procedure is used between the MME and the HSS and between the SGSN and the HSS to update location information into the HSS. The Update Location Request (ULR) is sent by the MME/SGSN to the HSS while the Update Location Answer (ULA) is sent by the HSS to the MME/SGSN.

  When the HSS receives an ULR message, it answers with an ULA with the subscriber data.
- Cancel Location Request/Answer (CLR/CLA)

  The Cancel Location procedure is used between the HSS and the MME and between the HSS and the SGSN to delete a subscriber record from the MME or SGSN. The Cancel Location Request (CLR) is sent by the HSS to the MME or SGSN
- Purge UE Request/Answer (PUR/PUA)

  The Purge UE procedure is invoked between the MME and the HSS and between the SGSN and the HSS to indicate to the HSS that a subscriber profile has been deleted from the MME or SGSN. This procedure can be invoked because the User Equipment has detached from the network. When the HSS receives a PUR message, it sets the MME flag or SGSN flag for the received IMSI as Purged and then sends a PUA message.
- Delete Subscriber Data Request/Answer (DSR/DSA)

  The Delete Subscriber Data Request (DSR) is used between the LTE-HSS and the MME and between the LTE-HSS and the SGSN to remove some or all data of the LTE-HSS user profile stored in the

MME or SGSN. The LTE-HSS sends a DSR when a GRPS/PDN context, Regional Subscription, APN configuration, CSG is deleted.

- Insert Subscriber Data Request/Answer (IDR/IDA) messages for Subscriber Data Handling Procedures.

  The Insert Subscriber Data Request (IDR) is used between the LTE-HSS and the MME and between the LTE-HSS and the SGSN for updating user Data in the MME or SGSN. When the EPS subscription is modified, the LTE-HSS sends an IDR message to the MME/SGSN if the user, for which the subscriber profile is modified, is attached.

- Reset Subscriber Request/Answer (RSR/RSA) messages for Fault Recovery Procedures.

  The LTE-HSS makes use of this procedure in order to indicate to the MME and SGSN that the LTE-HSS has restarted and may have lost the current MME-Identity and SGSN-Identity of some of its subscribers who may be currently roaming in the MME area and SGSN-Identity, and that the LTE-HSS, therefore, cannot send Cancel Location messages or Insert Subscriber Data messages when needed.

  The LTE-HSS sends a RSR after an LTE-HSS restart, if some IMSIs were attached before the LTE-HSS was killed.

- NotifyRequest/Answer (NOR/NOA) messages for Notification Procedures.

  The Notification Procedure is used between the MME and the LTE-HSS and between the SGSN and the LTE-HSS when an inter MME or SGSN location update does not occur but the LTE-HSS needs to be notified.

  When the LTE-HSS receives a NOR message, it answers with a NOA and stores the information coming for the NOR like the PDN GW Identity.

- Authentication Information Retrieval/Answer (AIR/AIA) for Authentication Procedures.

  The Authentication Information Retrieval (AIR) procedure is used by the MME and by the SGSN to request authentication information from the LTE-HSS. When the LTE-HSS receives an AIR message, it answers with an AIA message with authentication vectors computed in the Tekelec ngHLR's Authentication center.

To allow the Network Operator to configure the LTE-HSS and provision it with subscribers, the following entities have been implemented:

- LTE-HSS Configuration:
  - The new LTEHSSConfig entity allows to configure the LTE-HSS.
  - The LTE-HSS can accept incoming Diameter connections over TCP through several local IP addresses. The new LteHssConfigTCPListenAddress entity has been implemented to allow to configure the LTE-HSS with one or several local IP addresses, by adding new entries in the LteHssConfigTCPListenAddress entity.
  - The LTE-HSS can accept incoming Diameter connections over SCTP through several local IP addresses. The LteHssConfigSCTPListenAddress entity allows to configure the LTE-HSS with one or several local IP addresses, by adding new entries in the LteHssConfigSCTPListenAddress entity.
  - The new LteHssConfigDestinationHosts entity has been implemented in order to ultimately restrict the Diameter Peers that will be authorized to connect with the LTE-HSS, by defining a list of authorized diameter hosts in this entity.

  - The new LteHssConfigDestinationRealms entity has been implemented in order to ultimately restrict the Diameter Peers that will be authorized to connect with the LTE-HSS, by defining a list of authorized diameter realms in this entity.
  - The new HSSPLMN entity has been implemented in order to allow the Network Operator to define the Mobile Country Code and the Mobile Network Code for a range of IMSI. These definitions are used by the LTE-HSS to determine whether the subscriber is roaming in its HPLMN. Depending on the result and the subscriber's profile, the LTE-HSS will either allow or disallow the subscriber to roam in the current PLMN.

- LTE-HSS Subscriber Provisioning:
  - The new TemplatePDNContext entity has been implemented to allow the Network Operator to provision PDN Context Templates, which can then be linked in the subscriber profile at the creation time.
  - Several fields have been added in the HLR Subscriber Profile in order to take into account the PDN Context configuration. The following fields have been added to the HlrSubscriberProfile Entity: DefaultPdnContextId, SpPdnChargingCharacteristics, HlrProxyMode, AMBRUL, AMBRDL, APNOIReplacement, RFSPId.
  - The new ServiceProfilePDNContext entity has been implemented in order to allow the Network Operator to configure the PDN Context (GPRS Context for EPC Core network).
  - The new HlrSpPdnMipAgentInfo entity has been implemented to allow to configure the identity of the PDN-GW between the MME/SGSN and the LTE-HSS regardless of the specific mobility protocol used (GTP or PMIPv6).
  - The new SpecificAPNInfo entity has been implemented to allow the operator to view the list of active APNs stored by the MME or SGSN, including the identity of the PDN GW assigned to each APN.
  - Several fields have been added to the HlrVolatileData entity to allow the viewing of additional subscriber data: UrrpSgs, UrrpSgsn, HomogeneousSupp IMSVoiceOverPS Sessions, GMLCAddress, PSLCSNotSupportedByUE

Moreover, the following new operations have been implemented:

- `The ProxyLteUpLocToLegacyHlr()` operation under the LteMapOptions entity. When this new operation is invoked, the LTE-HSS sends a MAP-UL message on each ULR received from the MME/SGSN, for each subscriber for which the HlrProxyMode flag has been set to true („1) in its subscriber profile. This resynchronizes the legacy HLR if one MAP-UL has been lost between the HLR Proxy and the Legacy HLR.
- The LtePeersStatistics entity provides the following two operations to retrieve the list of connected diameters peers:
  - `GetPeerList()`

    This operation returns the full list of Diameter Peers (MME,SGSN, etc…) that are or have been connected to the LTE-HSS. It gives the Diameter Identities of the Peers, the type of connection used, the connection status and the number of time the Peer has been disconnected.
  - `GetConnectedPeers()`

    This operation returns the list of Diameter Peer that are currently connected to the LTE-HSS.

New LTE-HSS counters and alarms have been added, refer to the latest SDM Performance Measurements Rel6.2 and the latest SDM Alarm Dictionary Rel6.2 respectively for a more detailed description.

LTE-HSS features

Resource sharing with the Tekelec ngHLR

Tekelec's LTE-HSS runs on the SDM system. It shares the hardware, software, database and provisioning stream (OAM&P) with all the other applications running on the system, such as the Tekelec ngHLR.

This allows the LTE-HSS to use the Tekelec ngHLR's subscriber profile for mobility between 3G-LTE networks and Authentication Center for LTE authentication.

The LTE subscriber profile is integrated with the Tekelec ngHLR's subscriber profile, which means that they both share the same following data: volatile data, SIM, IMSI, GPRS contexts, etc. This also means that the LTE-HSS can manage multiple devices, multiple SIMs, multiple IMSIs and multiple identities scenarios.

HLR-proxy mode for bidirectional mobility between 3G and LTE networks

The LTE-HSS uses the SDM ngHLR's Authentication Center (AuC) in order to perform LTE authentication and also uses the SDM ngHLR's subscriber profile to support bidirectional mobility between the 3G-LTE networks.

LTE authentication

When a subscriber's SIM card is provisioned in the SDM's AuC with SIM Type= SIM or USIM, the LTE-HSS performs LTE authentication by using the SDM's AuC library (shared with the SDM ngHLR).

When a subscriber's SIM card is provisioned with SIM Type = Offboard (this SIM Type refers to a sim card hosted by an external legacy HLR), the LTE-HSS uses the SDM ngHLR's HLR-Proxy functionality to forward the authentication request to the legacy HLR to obtain authentication vectors from the subscriber's 3G legacy HLR.

To achieve this, the LTE-HSS is capable of converting a S6 AIR Diameter request into a Gr SAI MAP message and using the SDM ngHLR to proxy it to the correct 3G legacy HLR in order to retrieve authentication vectors. Note that this is transparent to the legacy HLR.

The SDM ngHLR in HLR-Proxy-Mode can then include those vectors into the S6 AIA message (and can also compute the KASME parameter on the fly in case of E-UTRAN authentication) as a response to the MME/SGSN's S6 AIR.

Mobility

The SDM system supports bidirectional seamless mobility between 3G-LTE networks in the following two scenarios:

- The subscriber has a 3G HLR profile provisioned in the SDM ngHLR and a 4G (LTE) profile provisioned in the LTE-HSS. The subscriber's ' HlrProxyMode' flag remains set to the default value ('false').

- The subscriber has a 3G HLR profile provisioned in an external legacy HLR and a 4G (LTE) profile provisioned in the SDM LTE-HSS. In this case, the subscriber's 'HlrProxyMode' flag should be set to 'true'.

Scenario 1

In the first scenario described above, the Location Update procedure is handled internally between the SDM ngHLR and the SDM LTE-HSS. When a subscriber's 'HlrProxyMode' flag is set to 'false' (default value), the subscriber is considered to be provisioned locally within the SDM database and the registration can be handled completely by the SDM system.

- Subscriber roaming from 3G to LTE networks in scenario 1 context:

  When the SDM receives an ULR message from the MME, its LTE-HSS retrieves the LTE subscriber data from its database and sends it back to the MME in a S6 ULA message. It also communicates internally with the SDM's ngHLR, which then sends out a MAP Cancel Location to the subscriber's previous 3G VLR/SGSN.

- Subscriber roaming from LTE to 3G networks in scenario 1 context:

  When the SDM receives a MAP UL message from the 3G VLR/SGSN, its Tekelec ngHLR retrieves the 3G subscriber data from its database and sends it back to the VLR/SGSN in a MAP ISD message. It also communicates internally with the SDM's LTE-HSS, which then sends out a S6 CLR message to the subscriber's previous MME.

Scenario 2

In the second scenario described above, the subscriber's profile is stored in an external legacy HLR and the 'HlrProxyMode' flag is set to 'true'. This means that the MAP Location Update procedure is handled by the SDM's HLR-Proxy and forwarded to the external legacy HLR. The LTE-HSS uses the SDM ngHLR's HLR-Proxy functionality in order to support bidirectional seamless mobility between 3G-LTE networks. The SDM HLR-Proxy functionality can support the necessary 3G mobility procedures (Update Location/Cancel Location, GPRS Update Location/GPRS Cancel Location, ISD, etc).

- Subscriber roaming from 3G to LTE networks in scenario 2 context:

  When the SDM receives an ULR message from the MME, its LTE-HSS retrieves the LTE subscriber data from its database and sends it back to the MME in a S6 ULA message. It also communicates internally with the SDM's HLR Proxy functionality, which then sends out a MAP Update Location to the legacy HLR, which perceives the SDM HLR Proxy as a SGSN and proceeds with the normal 3GPP UL procedure. The SDM's HLR Proxy forwarding a MAP UL to the legacy HLR ultimately incites the legacy HLR to send out a MAP Cancel Location to the subscriber's previous 3G VLR/SGSN.

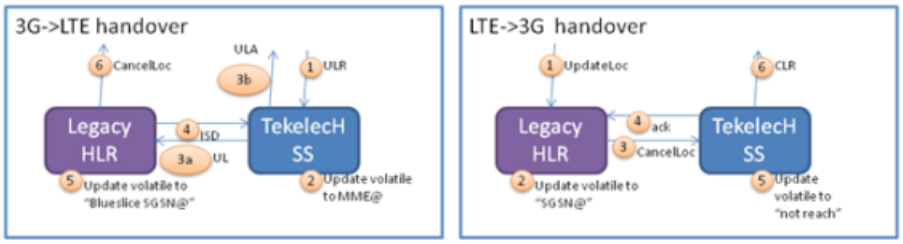
- Subscriber roaming from LTE to 3G networks in scenario 2 context:

  When the legacy HLR receives a MAP UL message from the 3G VLR/SGSN, it retrieves the subscriber's data from its database and sends back a MAP ISD to the VLR/SGSN, as per the normal 3GPP procedure. The legacy HLR then sends out a MAP Cancel Location to the SDM. The SDM's ngHLR communicates internally with the LTE-HSS, which in turn sends out a Diameter S6 Cancel Location Procedure (CLR) message to the previous MME.

As per example, hereunder are figures that show the message flow between the 3G/LTE network elements and Tekelec's LTE-HSS in some possible scenarios.

Example: Roaming between 3G and LTE networks

This example covers roaming between the 3G-LTE networks and vice versa within the context of scenario 2 as described above. This example is assuming the authentication has already been done.



Example: 3G>LTE Mobility

This example covers roaming between the 3G-LTE networks within the context of scenario 2 as described above. The subscriber's authentication credentials are stored in the legacy HLR.

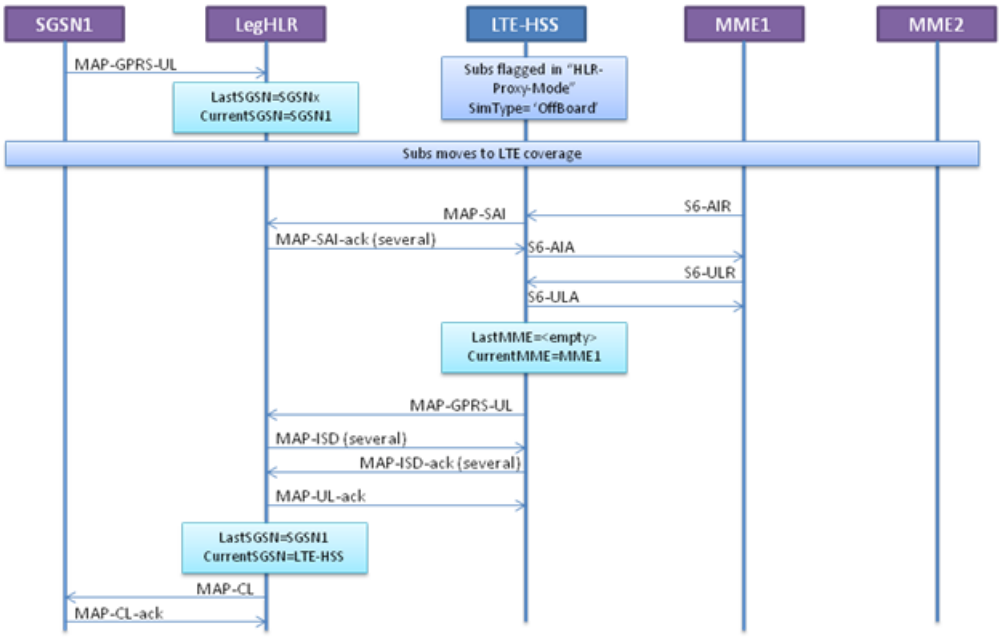


Figure 62: 3G>LTE Mobility

Example: LTE>3G Mobility

This example covers roaming between the LTE-3G networks within the context of scenario 2 as described above. This example is assuming the authentication has already been done.

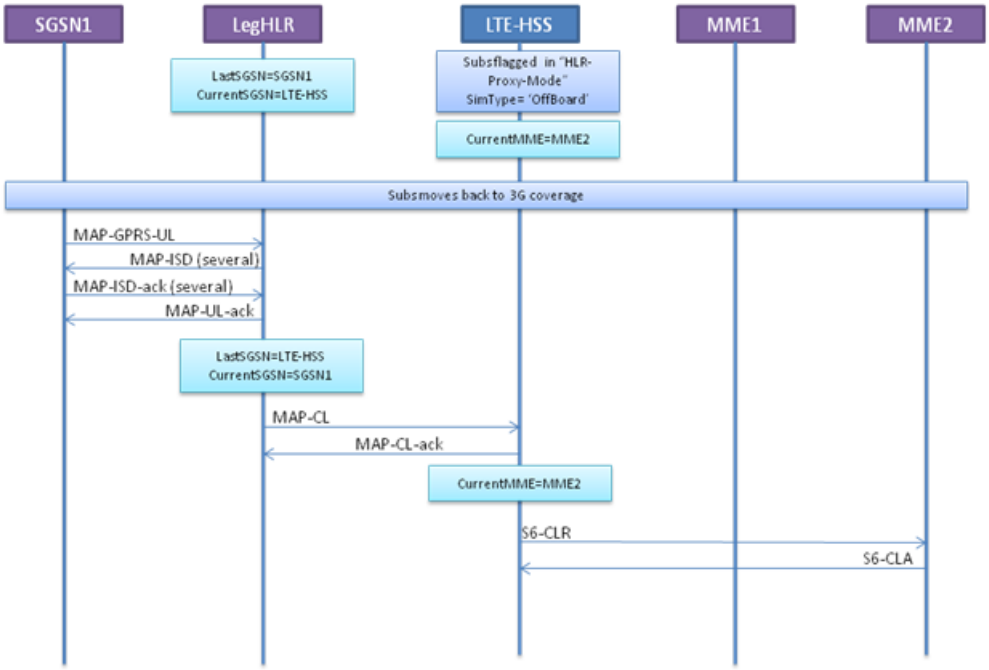


Figure 63: LTE>3G Mobility

Example: LTE>LTE Mobility

This example covers roaming within the LTE network in the context where the subscriber's LTE profile is stored in the SDM LTE-HSS.

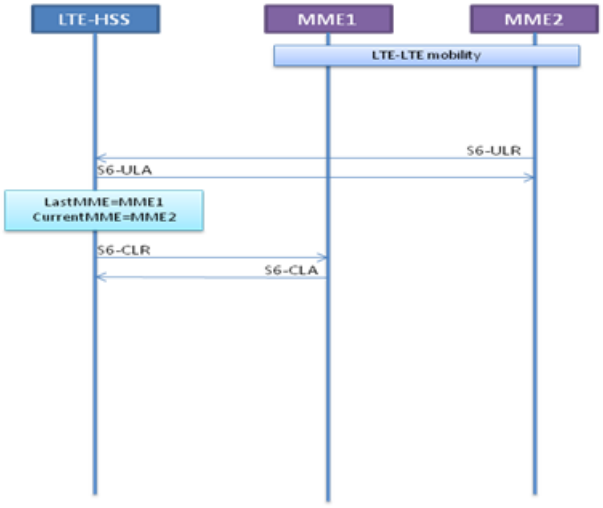


Figure 64: LTE>LTE Mobility

Compliance to 3GPP 29.272 v10.0.0

Tekelec made several smaller enhancements to LTE-HSS to align with 3GPP 29.272 v10.0.0. These enhancements affect Diameter messages, which carry a collection of attribute value pairs (AVPs)

containing an AVP code, length, flags and data. Some enhancements affect only the message field while others affect both the message field and the LTE-HSS behavior.

Enhancements to request/answer message types

Messages between the HSS and the MME or SGSN node provide additional information. The list shows the affected AVPs grouped by their message type.

- Update Location Request (ULR)
  - Active APN
  - GMLC Address
  - Homogeneous Support of IMS Voice-over-PS-Sessions
  - RAT Type
- Insert Subscriber Data Answers (IDA)
  - EPS User-State
  - EPS Location Information
  - IMS Voice-over-PS-Sessions Supported
  - Last-UE-Activity-Time
- Notification Requests (NOR)
  - PGW PLMN ID support

Enhancement Details

- **Active APN (Access Point Name)**

  The Active-APNs AVP contains information about a dynamically established APN, including the identity of the PDN GW assigned to each APN, on a serving node so the LTE-HSS can restore it if it is lost after a node restart. If the APN name is stored in the database, the LTE-HSS replaces the stored dynamic and specific PDN GW information with the information received in the list of Active APN AVPs. Specific PDN GW information is PDN GW information with a wildcard APN name "*".

- **EPS User-State/EPS Location Information**

  The EPS User State contains information related to the user state in the MME or the SGSN. EPS Location Information contains information related to the user location relevant for EPS. If the LTE-HSS receives a message from the Service Related Entity (SRE) requesting EPS User State or EPS Location Information, the HSS sets the "EPS User State Request flag" or the "EPS Location Information Request flag" as well as the "Current Location flag" in the IDR Request Flags.

- **Freeze P-TMSI/M-TMSI**

  If the HSS receives a PUR and the saved Diameter identities of the MME or SGSN for this IMSI are identical to the ones received in the PUR, the LTE-HSS returns a Purged UE Answer (PUA) with the flag "freeze M-TMSI" (MME) or "freeze P-TMSI" (SGSN). If the Diameter identities differ, the HSS returns a PUA without any PUA flags. When MME or SGSN receive the LTE-HSS response, it blocks M-TMSI or P-TMSI from immediate reuse.

- **GMLC Address**

  The GMLC-Address AVP contains the IPv4 or IPv6 address of the V-GMLC associated with the serving node V-GMLC address. This enhancement affects only the message field.

- **Homogeneous Support of IMS Voice-over-PS Sessions**

  This feature indicates whether "IMS Voice-over-PS Sessions" is supported homogeneously in all RAs and TAs currently associated to the serving SGSN. This information is part of an Update Location Request (ULR). there is no indication about the homogenous support of this function in all the serving nodes currently registered in HSS for the UE, the HSS sets the “T-ADS Data Request flag” (NOT_SUPPORTED (0), SUPPORTED (1)) in the IDR Request Flags.

- **IMS-Voice-Over-PS-Sessions-Supported**

  This feature indicates whether IMS Voice over PS Sessions is supported by the UE's most recently used TA or RA in the serving node. This information is part of an Insert Subscriber Data Answer (IDA). When receiving the IDR-Flags with the "T-ADS Data Request", the nodes return the time stamp of the UE's most recent radio contact, the associated RAT Type, and an indication of IMS Voice over PS support in the current (and most recently used) TA or RA.

- **PGW PLMN ID**

  The PGW PLMN ID identifies the PLMN in which the PDN GW is located. When the LTE-HSS receives a NOR, the LTE-HSS can either store PGW PLMN ID or replace it with the APN .

- **RAT-Type**

  The RAT-Type AVP identifies the radio access technology that is serving the UE at the time of the last radio contact. This enhancement affects only the message field.

- **Last-UE-Activity-Time**

  The Last-UE-Activity-Time AVP contains the point of time of the last radio contact of the serving node (MME or SGSN) with the UE. This enhancement affects only the message field.

Idle-Mode Signaling Reduction (ISR)

The Idle-Mode Signaling Reduction (ISR) feature provides significant signaling reduction through dual registration when a subscriber roams in an area where LTE and G3 networks are close together or overlap. Dual registration reduces the frequency of Tracking Area Update (TAU) procedures (LTE) and Routing Area Update (RAU) procedures (G3) as the subscriber keeps reselecting between these networks. The ISR feature also reduces internal network signaling.

For example, whenever a subscriber moves to a new MME tracking area (TA) or an SGSN routing area (RA), it triggers a TAU or RAU procedure, and each time de-registers itself from the MME or SGSN, to inform the LTE-HSS about its current location. A subscriber’s registration in both networks reduces the number of update procedures necessary to inform the LTE-HSS of a location change. MME and S4-SGSN can also communicate with each other and align their tracking area using the S4 interface.

MME and SGSN achieve dual registration by indicating to the LTE-HSS in an S6a/S6d Update Location Request (ULR) message to not cancel the location of the previous MME or SGSN. Based on the ULR-flags received and previous registration states, the LTE-HSS then replaces or adds the identities of the old MME or SGSN with the ones received in the request.

The MME or SGSN activates ISR only when it detects ISR support from the Serving GW. The network can activate ISR individually for each subscriber. When activated, the subscriber is registered with both MME and SGSN as well as LTE-HSS.

SGSN and MME may be implemented together, which reduces some interface functions but results also in some dependencies.

The ISR feature also interworks with the pre-R8 SGSN and with the HLR-Proxy mode. LTE subscribers that support G3 require ISR support.

Multiple registrations and LTE-HSS mobility behavior

Multiple registration can happen in two distinct situations:

1. The subscriber is registered by two separate nodes: an MME and an S4 SGSN, and the MME decides not to trigger Cancel Locations (CLR) toward the R8SGSN, for instance because of ISR.
2. The subscriber is registered twice, but with a combined MME/SGSN node. In this case, each node is treated as a separate node and has its own settings for answer message flags, but notifications (IDR,DSR and RSR) are sent only once.

The LTE-HSS differentiates both situations by using the SGSN number.

Figure 65: Mobility management services shows the LTE-HSS behavior and the triggered messages and states when the LTE-HSS receives a ULR message:

- The first column lists the current registration state for a given IMSI in the LTE HSS.

  Note: the non-standard additional case of a user being registered as a proxy to a 3G HLR is listed at the bottom of the table.

- The first row describes the received location management message, following this convention:
  - [Node type] / [Interface used to receive message] / [Type of Message] An additional row can be used to describe the use of eventual relevant flags.
- The content of the table describes the reaction of the LTE HSS toward the previously registered node, and the possible state maintained after a successful interaction.

Figure 65: Mobility management services

→ Node / Interface/ Location update message [flags] Currently registered node ↓	MME / S6a / ULR			SGSN / S6d / ULR		SGSN / Gr / UL	Combined MME-SGSN /S6ad / ULR	HLR / Gr / CL
	B5 Initial-attach-indicator	B0 Single-Registration indicator	B0 and B5 not set	B5 Initial-attach-indicator	B5 not set			
MME only	CLR	CLR	CLR	CLR	No CLR: Dual Registration	CLR	CLR	CLR
S4-SGSN only	CLR	CLR	No CLR: Dual Registration	CLR	CLR	CLR	CLR	CLR
SGSN only (pre-R8)	CL	CL	CL	CL	CL	CL	CL	N/A
Multiple Registration MME & S4-SGSN	CLR to both	CLR to both	CLR to MME only: Dual Registration	CLR to both	CLR to S4-SGSN only: Dual Registration	CLR to both	CLR to both	CLR to both
Combined MME/R8+ SGSN	CLR	CLR	CLR	CLR	CLR	CLR	CLR	CLR
HLR-Proxy registered	UL to HLR	UL to HLR	UL to HLR	UL to HLR	UL to HLR	N/A	UL to HLR	N/A

Examples:

- If the subscriber is registered only with an MME node and now enters the routing area of an SGSN node, the LTE-HSS does not send a Cancel Location Request message to the SGSN node to allow the subscriber also to register with the S4-SGSN.

- If the subscriber is registered only with the SGSN node and now enters the tracking area of an MME node, the LTE-HSS does not send a Cancel Location Request message to the MME node to allow the subscriber also to register with the MME node.
- If the subscriber is registered with a pre-Release 8 SGSN node, the LTE-HSS responds with a Cancel Location (CL).
- If the subscriber supports HLR-Proxy mode, the LTE-HSS responds to the HLR with an Update Location (UL) notification.

The Cancel Location Request (CLR) is sent by the HSS to the MME or SGSN when:

- A User Equipment is moving from one MME or SGSN area to another. There is an ongoing Update Location Procedure either from 4G to 4G network or 4G to 3G network.
- There is an initial Attach Procedure of the subscriber.

When a subscriber is disabled, no CLR is sent by the HSS to the MME and/or SGSN to which the Subscriber is registered.

Diameter Relay Agent

The Diameter Relay Agent feature allows the Diameter server node (HSS process) to accept Diameter connections from a Diameter Relay Agent and to make it able to send and receive Diameter far end messages coming through these Diameter Relay Agents. The HSS process includes IMS-HSS, IMS-SLF, LTE-EIR and LTE-HSS. A relay agent is advantageous because it can aggregate requests from different realms (regions) to a specific realm, which eliminates the configurations of network access servers for every Diameter server change.

When a DSR establishes a Diameter connection with a Diameter peer, the DSR sends first a Capability Exchange Diameter Request (CER). The diameter server node replies with a Capability Exchange Diameter Answer (CEA). During this exchange, the nodes determine their capabilities of supporting these application identities. When the HSS receives a CER with a compatible application identity, it tries to match this application with any locally supported applications, for example, S6, S13, Cx, or Sh. If no common application is found, the HSS rejects the CER and fails the diameter connection.

The Diameter Relay Agent feature is provisioned throughout the DraConfig table, which is common to IMS-HSS, IMS-SLF, LTE-EIR and LTE-HSS.

For more information about

- procedures to configure this feature, refer to the *SDM System Configuration – User Guide*.
- the table details, refer to the *SDM System Configuration – Reference Manual*.
- performance counters, refer to the *SDM Performance Measurements Manual*.

Subscription Profile Repository (SPR) Features

SPR functionality

The Tekelec Subscriber Data Server (SDS) is capable of taking on the SPR functionality by acting as a centralized system used for the storage of subscriber policy control data. The Tekelec SPR runs on the SDS and shares the hardware, software, database, and provisioning stream (OAM&P) with all the other applications running on the system (e.g., Tekelec ngHLR, SIP-AS, LTE-HSS). The Tekelec SPR

functionality can be supported on the EAGLE XG hardware platform (HP rackmount servers, HP c-Class server blades, and the PP-5160 (2 blades).

For an overview of the hardware used by SDM, refer to *Hardware description*. For a sample configuration and links to the HP user documentation, refer to the *SDM Roadmap to Hardware Documentation*. For TPD hardware/platform alarms, refer to the *SDM TPD Troubleshooting Guide*. And for details on the PP-5160, refer to the Policy Documentation set's PP-5160 *Hardware Installation Guide*.

The SPR can be deployed in environments where PCRF nodes need access to a separate repository for subscriber data and pool data acts as a centralized repository. This data includes:

- Subscriber:
  - Subscriber profile data: pre-provisioned information that describes the capabilities of each subscriber
  - Quota data: information that represents the subscriber's use of managed resources
  - DynamicQuota data: Storage of dynamic quota (roll-over, top-up, pass) limits
  - State data: subscriber-specific properties
- Pool:
  - Pool profile data: information about pool subscribers.
  - PoolQuota data: information about quota usage for the pool
  - DynamicPoolQuota data: information about dynamic quota for a pool
  - PoolState data: information about pool-specific properties

SPR call flows

The PCRFs can communicate with the SDM IMS-HSS front-end application over the Sh interface to write, query, or update the subscriber's policy data stored in the Subscriber Data Server. More precisely, the PCRFs can query User Profile data and can query or update Quota and State data using Sh transparent data mechanisms. To maximize performance on the PCRF-SPR interface, Sh Transparent data is stored by the SPR as a 'blob' (binary large object); however, access to specific fields within the profile 'blob' is provided through the XML provisioning interfaces.

The following Sh messages are used between the PCRFs and the SPR:

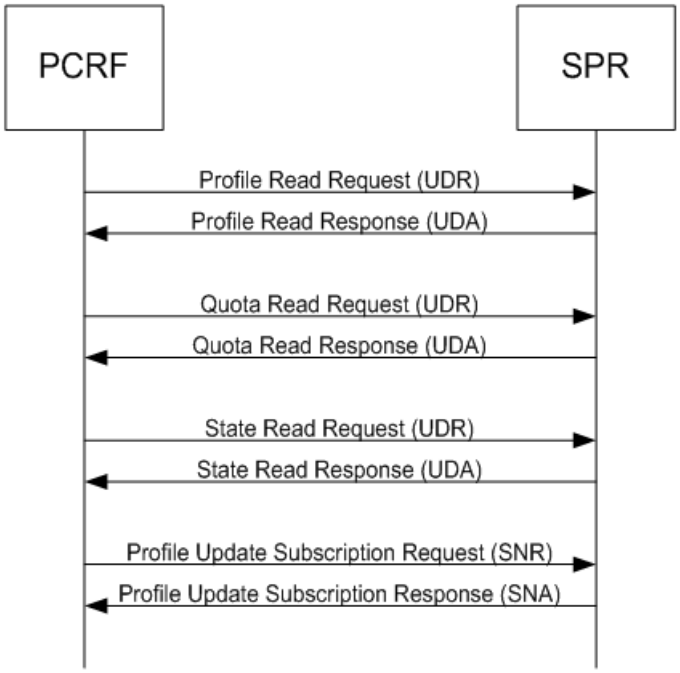
Table 28: Sh messages between PCRF and SPR

Message	Source	Destination	Description	Parameters
UDR	PCRF	SPR	User-Data-Request	User-Identity, Service-Indication
UDA	SPR	PCRF	User-Data-Answer	Result-Code, User-Data
PUR	PCRF	SPR	Profile-Update-Request	User-Identity, User-Data, Service-Indication
PUA	SPR	PCRF	Profile-Update-Answer	Result-Code
SNR	PCRF	SPR	Subscribe-Notifications-Request	User-Identity, Request-Type, Service-Indication
SNA	SPR	PCRF	Subscribe-Notifications-Answer	Result-Code, [User-Data]

PNR	SPR	PCRF	Push-Notification-Request	User-Identity, User-Data
PNA	PCRF	SPR	Push-Notification-Answer	Result-Code

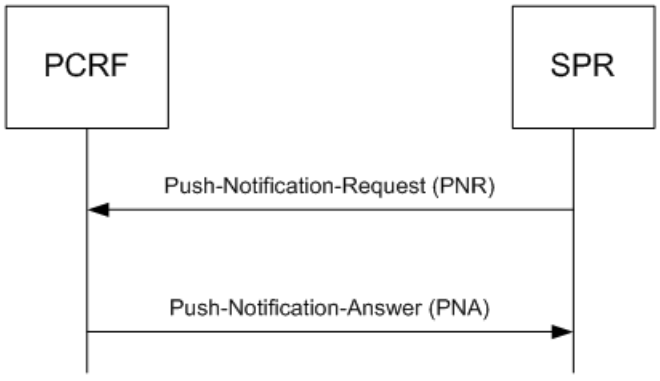
Session initiation

When a session is initiated, the PCRF retrieves policy profile data from the SPR. The PCRF may also subscribe to profile updates using the SNR message.



Mid-session event

The PCRF may receive updates from the SPR if the profile is updated during a session.

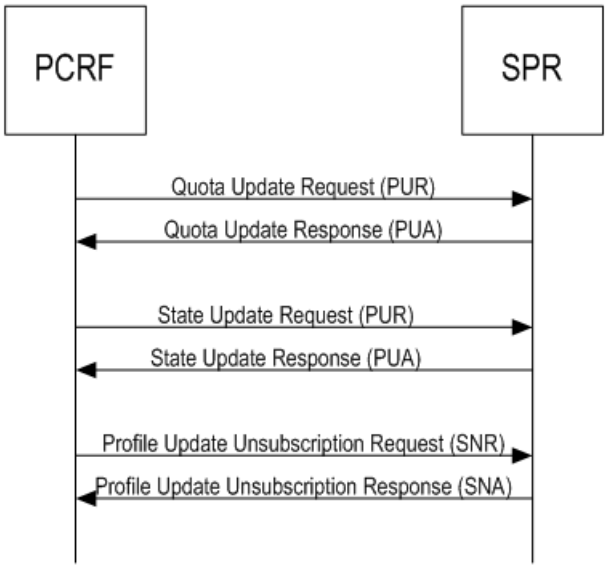


NOTE: By default, the SPR delays sending a PNR message for 5 seconds after a modification has been made to the user profile. In scenarios where multiple updates are made to a single subscriber profile, the delay ensures that the UDA message sent back to the PCRF includes the latest subscriber profile

information. The time delay is configurable through the HssConfig's HssHlrCommTmo attribute. See *HSS Configuration* in the *SDM System Configuration Reference Manual*.

Session termination

At the end of a session, the PCRF typically updates the user profile at the SPR level and unsubscribes from automatic profile updates.



SPR configuration and provisioning

To allow the Network Operator to configure the SPR and provision it with policy data, the following entities have been implemented:

- SPR Configuration:
  - The HssSPRServiceIndList (aka HssSPRServiceIndication) entity differentiates and maps the Service Indications that are sent by the PCRF in the Sh messages and the Service Indications that can be requested through the OAM (provisioning). At setup of the SPR functionality, the Tekelec *Customer Care Center* will load the following Service Indications into the system: CamiantQuotaData, CamiantStateData, CamiantUserData. The entity allows the following:
    - The IMS-HSS to act as a true performant SPR by storing the data received from the PCRF in the database independently from all other IMS-HSS data.
    - The User Data to be encrypted in the database.
  - The HssSystemOptions entity allows the Network Operator to dynamically
    - Turn On/Off the SPR functionality's Auto-Enrollment feature. This feature can be useful where the subscriber profiles are initially stored outside of the SPR. For more details on this feature, refer to *SPR Diameter Sh Auto-Enrollment on PUR*.
    - Set the compression level the IMS-HSS must use when storing the Service Data in the database.

For more information on the configuration entities that have been implemented for the SPR functionality, refer to the *Configuration entities for the IMS-HSS's SPR functionality* section of the *SDM*

System Configuration - Reference Manual. For more information on how to configure/troubleshoot these entities from the WebCI, refer to the *Configuring the IMS-HSS's SPR functionality* section of the *SDM System Configuration - User Guide*.

- SPR Provisioning:
  - The Subscriber (alias Policy) entity allows the Network Operator to provision/manipulate policy data in the SPR.

For more information on the Subscriber provisioning entity, refer to the "Subscription Profile Repository (SPR)" chapter of the *SDM Subscriber Provisioning - Reference Manual*. For more information on how to provision policy profiles using XML interfaces, and for samples of XML scripts, refer to the *SDM Subscriber Provisioning - User Guide*. For instructions on how to view policy profiles (profile data, quota, state) and how to manipulate/troubleshoot the policy profile data from the WebCI, refer to the "Viewing/Editing Policy Profiles" section of the *SDM Monitoring, Maintaining, Troubleshooting-User Guide*.

The policy profile is provisioned as relation data. It is used to identify a subscriber using one of the following keys:

- AccountId
- Imsi
- Msisdn
- NAI (user@domain)

The provisioning interfaces listed hereunder support either one or both the provisioning/manipulation of the policy profiles in the SPR (for more details on which interface can be used for which type of action, refer to the "Subscription Profile Repository (SPR)" section of the *SDM Subscriber Provisioning-Reference Manual*):

- XML/TCP Interface (aka as Direct XML).
- XML/SOAP interface
- CLI
- WebCI
- XML-REST Interface (aka as the MSR API)
- LDAP Interface (only used for queries)

With the proper configuration, the IMS-HSS can act as an SPR and handle the policy profile as an IMS-HSS profile if a SubscriptionID and PublicIdentity are defined.

The SPR allows a PCRF to read/write/subscribe to Transparent Data when using one of the following identity keys in the Sh messages:

- MSISDN
- NAI (user@domain)
- IMSI

Any of these identity keys can be set as the primary key in the configuration of the system. The primary key can be configured at installation of the system. By default, the primary key is MSISDN and if you wish to set the IMSI or NAI as the primary key, contact the Tekelec *Customer Care Center*.

The SPR then converts the configured primary key into an Sh Identity using 3GPP standard 23.003 (see 13.3 for IMSI and 13.4 for NAI/MSISDN).

Clients of the XML-REST and LDAP interfaces can access the database using the MSISDN, NAI, IMSI, or AccountId. Clients of the XML/TCP or XML/SOAP interfaces can access the database using the SubscriptionID, IMPU, AccountId, IMSI, MSISDN, or NAI.

The figure of the SPR Data Model depicts the different provisioning interfaces. Note that in the figure, the MPE plays the role of a PCRF.

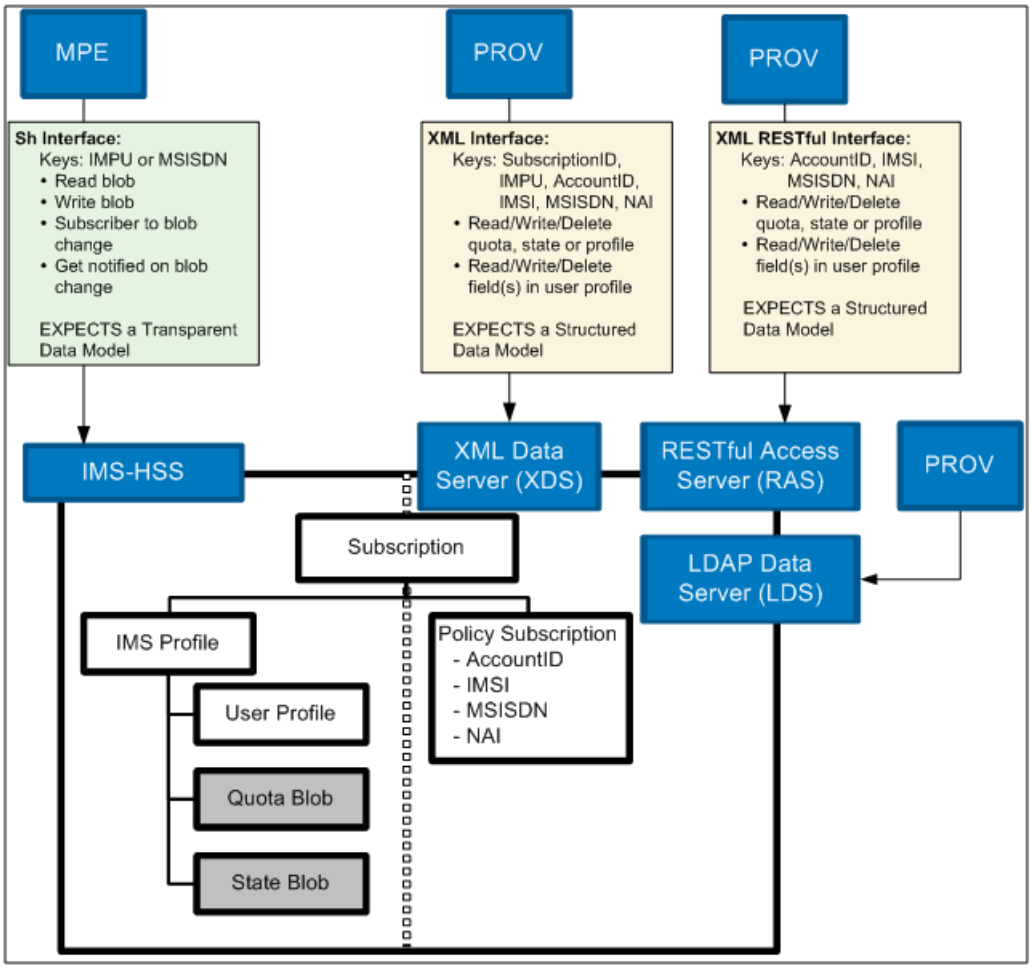


Figure 66: SPR Data Model

SPR Diameter Sh Auto-Enrollment on PUR

The SH Auto-Enrollment feature can be turned On/Off in the IMS-HSS's configuration (see the HssSPRConfig entity in the SDM System Configuration-Reference Manual). The PURAutoEnrollment flag is for the Sh Auto-Enrollment on PUR feature.

This feature becomes useful in the cases where the subscriber profiles are initially stored outside of the SPR. In such systems, only the Quota and State data is stored in the SPR.

When turned **On**, this feature allows the SPR to receive a Sh PUR request for an un-provisioned subscriber. Upon reception of such a request for an un-provisioned subscriber, the SPR automatically provisions a policy profile with all mandatory keys and populates the transparent data as per PUR inputs.

This allows the SPR to store the repository data received in the PUR request for an un-provisioned User Identity and later to be able to receive UDR/SNR requests for this subscriber.

When turned **Off**, upon reception of a Sh PUR request for an un-provisioned subscriber, the SPR sends back a `DIAMETER_ERROR_USER_UNKNOWN` answer and rejects the request.

The auto-enrollment feature can be dynamically turned On/Off from the CLI or WebCI, by setting the HssSPRConfig entity's PURAutoEnrollment flag. For instructions on how to do so from the WebCI, refer to the "Configuring the IMS-HSS's SPR functionality" section of the *SDM System Configuration - User Guide*.

Two SPR counters are used to collect PUR Auto-Enrollment data (refer to the latest *SDM Performance Measurements* for more details on the counters): Number of successful auto-enrollment and Number of failed auto-enrollment. They respectively count the number of successful/failed attempts at automatically creating profiles upon reception of Sh PUR with quota and state information for an un-provisioned subscriber.

Note: Only Sh PUR messages with the Data Reference AVP set to Repository-Data is handled in this manner:

On receiving a PUR message, the server queries the database to see if the User Identity contained in the message is present (only distinct User Identity attributes are handled, not wildcard). If the User Identity is not found in the database and the PUR Auto Enrollment feature is enabled (turned **On**), the server attempts to create a new subscription (SubscriptionID and profile) for the user. If all the required entries are successfully created for the new subscription, the received PUR request is processed normally.

The IMS Public User Identity used for the subscription is the User-Identity attribute received in the PUR message.

The SubscriptionID is created by extracting information from the User Identity AVP received in the PUR message as follows:

- If the User Identity follows a SIP URI based on an IMSI format: (where: ABC is the mnc value and XYZ is the mcc value), the Subscription ID will be the entire SIP URI.
- If the User Identity follows a TEL URL based on a MSISDN format: , the Subscription ID will be the entire TEL URI.
- If the User Identity follows a NAI based on username format: , the Subscription ID will be the entire NAI.

If an error is detected during processing, (i.e., no entry exists in the HssAuthorizedVisitedNetworks entity), then the transaction is rolled back, no entry is populated for the subscription, the repository data is not saved and a PUA with `DIAMETER_UNABLE_TO_COMPLY` answer is returned to the PCRF.

SPR XML-REST/XML/SOAP Auto-Enrollment

The XML-REST/XML/SOAP auto-enrollment feature can be turned On/Off in the IMS-HSS's configuration (see the HssSPRConfig entity in the SDM System Configuration-Reference Manual). The XMLAutoEnrollment flag is for the XML-REST/XML/SOAP Auto-Enrollment feature.

This feature becomes useful in the cases where the subscriber profiles are initially stored outside of the SPR. In such systems, only the Quota and State data is stored in the SPR.

When turned **On**, this feature allows the SPR to receive a XML-REST/XML/SOAP request for an un-provisioned subscriber. Upon reception of such a request for an un-provisioned subscriber, the

SPR automatically provisions a policy profile with all mandatory keys and populates the transparent data as per XML-REST/XML/SOAP inputs.

This allows the SPR to store the repository data received in the XML-REST/XML/SOAP request for an un-provisioned User Identity and later to be able to receive UDR/SNR requests for this subscriber.

When turned **Off**, upon reception of a XML-REST request, the SPR sends HTTP 404 (Not Found) with MSR 4001. When turned **Off**, upon reception of XML/SOAP request, the SPR sends mysql Error code 1032 (can't find record in) within the response.

The XML auto-enrollment feature can be dynamically turned On/Off from the CLI or WebCI, by setting the HssSPRConfig entity's XMLAutoEnrollment flag. For instructions on how to do so from the WebCI, refer to the "Configuring the IMS-HSS's SPR functionality" section of the SDM System Configuration – User Guide.

On receiving a REST message, the server queries the database to see if the KeyValue contained in the HTTP URI is present. If the KeyValue is not found in the database and the XMLAutoEnrollment feature is enabled, the SPR implements the enhanced XML auto-enrollment logic and creates a subscriber profile.

On receiving a XML/SOAP message, the server queries the database to see if the key attribute from the Update command is present. If the key attribute is not found in the database and the XMLAutoEnrollment feature is enabled, the SPR implements the enhanced XML auto-enrollment logic and creates a subscriber profile.

The SubscriptionID is created by extracting information from the KeyType/KeyValue received from the REST message as follows:

- If the KeyType is IMSI and KeyValue follows an IMSI format: IMSI, the Subscription ID will be sip: IMSI@ims.mncXYZ.mccABC.3gppnetwork.org.
- If the KeyType is MSISDN KeyValue follows a MSISDN format, e.g. +5149359700, the Subscription ID will be tel: +5149359700.
- If the KeyType is NAI and KeyValue follows a NAI format: UserName@example.com, the Subscription ID will be sip:UserName@example.com,.

Note: the KeyType should match the key type defined in SPR system. Only one key type is defined at a time in the system.

SPR Diameter Sh Auto-Enrollment on SNR

The SNR auto-enrollment feature is turned On/Off in the IMS-HSS's configuration (see the HssSPRConfig entity in the SDM System Configuration-Reference Manual). The SNRAutoEnrollment flag is for the Auto-Enrollment on SNR feature.

On receiving a SNR for such a subscriber the SPR creates a policy profile and registers the PCRF to receive notifications of changes to the subscriber's profile.

This feature allows the SPR to receive a SNR (Subscriber Notification Request) from a subscriber when no SPR Profile data exists. A SNR is a message on the Diameter Sh Interface that is sent from a PCRF to an SPR to register the PCRF (Policy and Charging Rules Function) to receive notifications whenever the policy data for a subscriber is modified. On receiving a SNR for such a subscriber, an auto-enrollment is performed, creating a SPR Profile entry for the subscriber. The SNR auto-enrollment entry values included for a subscriber are the Subscription Id, Public Identity, Service Indication and one of MSISDN, IMSI or NAI.

After a successful auto-enrollment, the subscriber is registered, normal SNR processing resumes, and an entry is inserted into the database. This database entry includes the identity of the subscriber , the service indication of the subscriber, and the address of the PCRF that is notified when the subscriber data is modified. The created profile includes a minimal amount of data to uniquely identify the subscriber. Whenever user data for a registered subscriber is modified a Sh Notification (PNR) is sent to all PCRFs registered to receive notifications of changes to that subscriber's data.

The auto-enrollment feature is only applicable to SNR with the DataReference AVP set to REPOSITORY_DATA and ServiceIndication AVP with values consisting of service-identities that match an entry in the configurable SPR Service Indication list.

On receiving a SNR message, the server queries the database to see if the User Identity contained in the message is present (only distinct User Identity attributes are handled, not wildcard). If the User Identity is not found in the database and the SNR Auto Enrollment feature is enabled (turned **On**), the server attempts to create a new subscription (SubscriptionID and profile) for the user. If all the required entries are successfully created for the new subscription, the received SNR request is processed normally.

The SPR Auto-Enrollment on SNR feature can be dynamically turned On/Off from the CLI or WebCI, by setting the HssSPRConfig entity's SNRAutoEnrollment flag. For instructions on how to do so from the WebCI, refer to the *Configuring the IMS-HSS's SPR functionality* section of the *SDM System Configuration – User Guide.*

If an error is detected during processing, the transaction is rolled back, no entry is populated for the subscription, the repository data is not saved, and a SNA with `DIAMETER_UNABLE_TO_COMPLY` answer is returned to the PCRF.

SPR Cleanup of Auto-Enrolled Profiles

The SPR Cleanup of auto-enrollment feature is turned On/Off in the IMS-HSS's configuration (see the HssSPRConfig entity in the SDM System Configuration-Reference Manual). The AutoEnrollmentCleanup flag is for the SPR Cleanup of Auto-Enrolled Profiles feature.

This feature provides a mechanism for service providers to automatically delete auto-enrolled subscribers from the database when these subscribers become inactive. This feature provides a means of removing profile records in 2 situations.

Automatic Cleanup Removes auto-enrolled profiles when a SNR de-register is received for a subscription and there are no other subscriptions registered for the profile.

When receiving a SNR for subscription de-registration, the source flag of the profile is examined, and if the profile was created by auto-enrollment and there are no other subscriptions for the same profile, the profile and all associated data for the user are removed from the database. The removed data includes the SPR repository data, any notification subscriptions registered on that data, and the subscription and identity keys associated with the profile.

Periodic Cleanup Removes auto-enrolled profile records when a specified period of inactivity is passed.

A time-stamp (ActiveSubsTimeStamp) associated with auto-enrolled SPR profiles is used to record the time of the latest update activity performed on the profile records for a subscriber. The TimeoutOfAutoEnrolledPolicy attribute is used to specify the allowable period of inactivity for an auto-enrolled profile after which the profile is deemed to be inactive. A periodic checking of the inactivity period of all auto-enrolled profile data is performed on a scheduled interval. If, on periodic checking, the period

of inactivity exceeds a configured time value (timestamp plus allowable inactivity value is less than the current time), the profile and all associated data is removed from the database. The removed data includes the SPR repository data, any notification subscriptions registered on that data, and the subscription and identity keys associated with the profile.

The SPR cleanup of Auto-Enrolled Profiles feature is only applicable to SNR with the DataReference AVP set to Unsubscribe and the specified subscription is the last subscription remaining on the subscriber's policy data.

The configuration parameters associated with the periodic checking and removal of auto-enrolled profiles include:

AutoEnrollmentCleanup	Used to enable and disable the cleanup feature and can be set to **On** or **Off**. The default is **Off**.
TimeoutOfAutoEnrolledPolicy	States the number of days that an auto-enrolled policy remains inactive before being removed. The default value is **60** days.
PeriodicCheckStartTime	The time of day that the periodic check for inactive policies is run. The default is midnight (**00:00:00**).
CheckingPeriod	The number of days (**0**-**90**) between execution of the periodic check. A value of **0** disables the periodic check. The default value is **0**.

The SPR Cleanup of Auto-Enrolled Profiles feature can be dynamically turned On/Off from the CLI or WebCI, by setting the HssSPRConfig entity's AutoEnrollmentCleanup flag. For instructions on how to do so from the WebCI, refer to the *Configuring the IMS-HSS's SPR functionality* section of the *SDM System Configuration – User Guide.*

Subscription Profile Repository data compression

The SPR is capable of compressing the Policy User Data before storing it into the database. At installation, the Tekelec *Customer Care Center* configures the HssSPRServiceIndication entity with Service Indications, which allows the IMS-HSS to act as a true performant SPR, by:

- storing the data received from the PCRF in the database, independently from all other IMS-HSS data.
- encrypting the User Data in the database.

The SPR encrypts User Data in the database, by using the zlib compression algorithm, as per the RFC1950. The compression levels can be configured dynamically by the Network Operator from the CLI or WebCI, by setting the SPRRepDataCompressionLevel parameter in the HssSPRConfig entity, with values ranging from 0 (No Compression) to 9 (Best Compression).

For more information on the HssSPRConfig entity, refer to the "Configuration entities for the IMS-HSS's SPR functionality" section of the *SDM System Configuration - Reference Manual*. For more information on how to configure/troubleshoot this entity from the WebCI, refer to the "Configuring the IMS-HSS's SPR functionality" section of the *SDM System Configuration - User Guide*.

SPR in Multi-Key Access Networks

The SPR in Multi-key Access Networks feature enables the Sh interface to access and provision a subscriber of multiple networks by any one of these provisioned subscriber access keys:

1. MSISDN
2. IMSI
3. NAI
4. Account Id

For example, a subscriber may be part of a wireless network using the MSISDN as access key as well as a WiMax network using the Network Access Identifier (NAI) as access key. All the information is stored in the same subscriber profile.

For a subscriber that becomes auto-enrolled, the Sh auto-enrollment function creates a subscriber profile using the public identity provided in the Sh request. The Public Identity is derived from an association of the identity type and its subscriber identity. For example, the subscriber identity `19194605500` of ID type MSISDN becomes public identity `Tel:19194605500`. The table shows the Public Identity structures for MSISDN, IMSI, and NAI.

ID Type	Subscriber ID	Public ID Structure	Public ID Example
MSISDN	19194605500	Tel:<msisdn>	Tel:19194605500
IMSI	19876543210	SIP:<imsi>@<network code>.<country code>.3gppnetwork.org	SIP:19876543210@ims.mnc076.mcc198.3gppnetwork.org
NAI	user@domain.com	SIP:<nai>	SIP:user@domain.com

The subscriber data is accessible only through the same public identity that was provided in the Sh message. A different identity would automatically create a new subscriber profile.

Identifier types can be created when creating the profile or at a later time. When an identity type is removed from the profile, the association is also removed.

Subscriptions for notifications of subscriber data changes apply to a specific identity type. When subscriber data changes, a notification is sent for each identity type for which the subscriber has registered a subscription.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

This feature requires provisioning only if additional access keys shall be provisioned in the Subscriber profile. Refer to *Table 29: Provisioning Information - SPR in Multikey Access Networks* to locate Subscriber provisioning information for identity keys.

Table 29: Provisioning Information - SPR in Multikey Access Networks

Affected Components	Description	Reference
Provisioning Interfaces	CLI, WebCI, XML interfaces: XML (TCP/SOAP), XML-REST	*Product Description*
Entities[], important attributes	Subscriber[], MSISDN, AccountId, IMSI, NAI	*SDM Subscriber Provisioning Reference Manual*

Affected Components	Description	Reference
Alarms	None	---
Error Messages	None	---
Counters	None	---
Procedures	• *Viewing/Editing Subscriber (Policy) Profiles (WebCI)*	*SDM Monitoring, Maintenance, Troubleshooting User Guide*
	• *SPR Subscriber Provisioning Templates (XML)*	*SDM Subscriber Provisioning User Guide*

Quota Editing via SDM API

The SPR *Quota Editing via SDM API* feature allows the operator to edit the quota fields within a quota of a specific subscriber. These fields can be accessed through the XML interfaces as well as WebCI and CLI.

The Quota data provides information about the subscriber's use of available resources. This data is stored in the subscriber profile in the form of an XML string (blob). To access the fields, the XML interfaces use the Quota name and any of the key values stored in the subscriber profile, that is, MSISDN, NAI, IMSI, or AccountId. WebCI and CLI can access these fields only through the Public Identity key.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 30: Provisioning Information - Quota Editing

Affected Components	Description	Reference Location
Provisioning Interfaces	CLI, WebCI, XML interfaces: XML (TCP/SOAP), XML-REST	*Product Description*
Entities[], attributes	• `QuotaEntity[]` (Subscriber Quota), `Name, Time, TotalVolume, InputVolume, OutputVolume, ServiceSpecific, NextResetTime, Type, GrantedTotalVolume, GrantedInputVolume, GrantedOutputVolume, GrantedTime, GrantedServiceSpecific, QuotaState,` • `Subscriber[]` (stores MSISDN, AccountId, IMSI, NAI)	*SDM Subscriber Provisioning Reference Manual*

Affected Components	Description	Reference Location
Alarms	None	---
Error Messages	• `1022 DupKey` • `1032 KeyNotFound` • `1054 BadFieldError` • `2010 InvalidValue` • `7004 OampInvalidRequest` • `7013 OampGeneralFailure`	*SDM Monitoring, Maintenance, Troubleshooting Reference Manual*
Counters	None	---
Procedures	• *Viewing/editing a subscriber quota (WebCI)* • *Viewing/editing subscriber (policy) profiles*	*SDM Monitoring, Maintenance, Troubleshooting User Guide*
	• *Subscriber Quota provisioning templates (XML)* • *Subscriber Quota provisioning templates (XML-REST)*	*SDM Subscriber Provisioning User Guide*

SPR Support for Pooled Quota

The SPR Support for Pooled Quota feature allows the Subscriber Provisioning Repository (SPR) to store and manage the shared quotas of a subscriber.

A quota restricts a subscriber to a specified amount of data volume, active sessions, or service-specific events. By pooling quotas, subscribers can share their resources.

Each subscriber can be part of only one pool. All pool subscribers share the pool information. The Network Operator can view pool information through the unique PoolID or any of the member subscriber identities (MSISDN, IMSI, NAI, or Account Id).

This feature also defines the service indications that are sent by the PCRF in the Sh messages as well as those that can be requested through the OAM and are then associated with the service indications provided in the Sh messages.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 31: Provisioning Information - Pooled Quota

Affected Components	Description	Reference
Provisioning Interfaces	CLI, WebCI, XML interfaces: XML (TCP/SOAP), XML-REST	*Product Description*

Affected Components	Description	Reference

Entities[], attributes	• Subscriber[]
	• `QuotaEntity[]` (Subscriber Quota), `Name, Time, TotalVolume, InputVolume, OutputVolume, ServiceSpecific, NextResetTime, Type, GrantedTotalVolume, GrantedInputVolume, GrantedOutputVolume, GrantedTime, GrantedServiceSpecific, QuotaState,`
	• QuotaState[]
	• Pool[]
	  • PoolQuota (blob, read-only)
	  • PoolState (blob, read-only)
		SDM Subscriber Provisioning Reference Manual

	• HssSPRServiceIndicationt[]:
	  • Pool <-> CamiantPoolData
	  • PoolQuota <-> CamiantPoolQuota
	  • PoolState <-> CamiantPoolState
		SDM System Configuration Reference Manual

Alarms	None	---
Error Messages	`7055 - SprPoolHasSubscriber`	*SDM Monitoring, Maintenance, Troubleshooting Reference Guide*
Counters	None	---
Procedures/ Templates	• *Viewing/editing subscriber (policy)profile* • *Viewing/editing subscriber quota* • *Viewing/editing SPR pool information (WebCI)*	*SDM Monitoring, Maintenance, Troubleshooting User Guide*
	• *SPR Pool provisioning templates (XML)* • *SPR Pool provisioning templates (XML-REST)*	*SDM Subscriber Provisioning User Guide*
	To map service indications (WebCI): • *Configuring SPR Service Indications*	*SDM System Configuration User Guide*

SPR support for Pass Management

The *SPR support for Pass Management* feature enhances the *Pooled Quota* feature by allowing overwrites to the basic quota allowance through Passes (one-time overwrite), Top-ups (modified plan), and Roll-overs (credits). These quota types are available for subscriber and pool data.

The network operator can provision these quota types to change dynamically using the DynamicQuota or the PoolDynamicQuota attribute. For the SPR, DynamicQuota and PoolDynamicQuota data are read-only (opaque data), that is, the data is stored as an XML string but will not be interpreted by the SPR. See also *Communication between MPE and SPR*.

The service indications used to send usage information are mapped as follows:

- DynamicQuota > CamiantDynamicQuotaData
- PoolDynamicQuota > CamiantPoolDynamicQuotaData

Pass

A Pass is a one-time override, which temporarily replaces or augments the subscriber default plan or service. While a Pass is in effect, it may modify the Quality of Service (QoS) controls, charging parameters, or other configurable rules associated with a subscriber service. A Pass may be valid for a restricted interval, continuously, apply to the subscriber or pool overall usage, or similar scenarios.

Passes are common options for pre-paid subscribers, who frequently have limited or no data access via their basic plan, and may purchase Passes to gain access to such services. They can also be used to allow Casual Use plans for pre- or post-paid subscribers to purchase services on an occasional basis, for which they would not otherwise subscribe on an ongoing basis.

Top-up

A Top-up is a modifier, which takes effect only upon exhaustion of basic Quota associated with a subscriber plan or default service. Top-ups allow the subscriber to extend the access to services beyond the time or volume limits typically enforced.

For example, a subscriber has a plan that allows 500 SMS messages per month. Twenty days into the month, 480 messages have been sent. The subscriber purchases three top-ups for 50 additional SMS messages.

Roll-over

A Roll-over is a mechanism by which usage that was not consumed during one Quota period may be applied as a credit in a future period. Roll-over may apply to basic Quotas associated with a subscriber Plan, or may affect Passes or Top-ups purchased by the subscriber. Roll-overs may be limited to the amount that can be credited to the future period, or by capping the total amount of (basic and rolled-over) credit that may be available in a given period. Roll-overs may also have limitations regarding the number of cycles that credits may be rolled into, that is, roll-over rules modify the process of resetting a recurring Quota.

For example, a roll-over may allow a subscriber to save up to 50% of their daily minutes, but only until the next day. Rollover units are consumed before regular plan units.

The default roll-over information comes from the MPE and may be overwritten by the provisioned roll-over information from the SPR. When the MPE requests usage information from the SPR to perform rollover calculations, the MPE updates the usage data and returns it to the SPR.

Communication between MPE and SPR

Top-up and roll-over information (dynamic quota) is shared between the SPR and MPE servers. The default information comes from the MPE and may be overwritten by the provisioned usage information from the SPR. The usage information is stored in the SPR DynamicQuota table. When the MPE requests usage information from the SPR, the SPR sends the usage information to the MPE using the CamiantDynamicQuotaData service indication in the following Diameter messages:

- UDA (User-Data-Answer): Sent in response to a UDA
- SNA (Subscribe-Notification-Answer)

The MPE updates the usage information and sends it to the SPR using CamiantDynamicQuotaData service indications in the following Diameter message:

- PUR (Profile-Update-Request)

The MPE deletes the dynamic quota information when a top-up becomes exhausted or expired; or there are no roll-over units to roll over. Top-ups cannot be rolled over.

The information for a Pass comes from three different locations. The Network operator defines the default values in the Policy CMP. The SPR provides the provisioned information (e.g., overrides) and the usage information, which is then recorded by the MPE for each Pass.

Provisioning

When provisioning Roll-overs, the Network Operator can specify the initial values granted for:

- time rolled over
- input, output, and total volumes
- number of service-specific units

When provisioning Passes and Top-ups, the Network Operator can:

- Specify preferences of one pass or top-up over another (priority)
- Specify an initial set of units (on CMP) and then override it for a specific subscriber (by SPR)
- Specify a pass or top-up to be expired at a specific date/time (Expiration Date/Time)
- Prevent a pass or top-up from being used until after a specific date/time (activation time)
- Force a pass or top-up to be consumed within a specified time of first use (duration)

A Pass cannot use top-ups.

Provisioning information

This section identifies affected provisioning components for this feature and the location of additional information.

Table 32: Provisioning Information - Pass Management

Affected Components	Description	Reference
Provisioning Interfaces	CLI, WebCI, XML interfaces: XML (TCP/SOAP), XML-REST	*Product Description*

Affected Components	Description	Reference
Entity[]/ attributes	Dynamic quota information: • `Subscriber[]/DynamicQuota` (blob)	*SDM Subscriber Provisioning Reference Manual*, SPR entities, Subscriber
	Pool dynamic quota information: • `Pool[]/PoolDynamicQuota` (blob)	*SDM Subscriber Provisioning Reference Manual*; SPR entities, Pool

	Service indications:
	• HssSPRServiceIndication[]
	  • DynamicQuota <-> CamiantDynamicQuota
	  • PoolDynamicQuota <-> CamiantPoolDynamicQuota
		SDM System Configuration Reference Manual, HSS SPR Service Indication List

Alarms	None	---
Error Messages	None	---
Counters	None	---

Procedures/ Templates	To add or update dynamic quota (blob):
	• *Add/update a dynamic quota*
	  • specify dynamic quota type, name, and priority over each other (`Type, Name, Priority`)
	  • specify granted initial values (`InitialTime, InitialTotalVolume, InitialInputVolume, InitialOutputVolume, InitialServiceSpecific`)
	  • specify date/time for quota activation, expiration, or duration (`ActivationDateTime, ExpirationDateTime, Duration`)
	
	To display dynamic quota:
	• *Display DynamicQuota by MSISDN*
		SDM Subscriber Provisioning User Guide
		• SPR subscriber provisioning templates (XML)
		• SPR subscriber provisioning templates (XML-REST)

Affected Components	Description	Reference

	To add or update pool dynamic quota (blob):
	• *Add/update a pool dynamic quota*
	  • specify pool dynamic quota type, name, and priority over each other (`Type, Name, Priority`)
	  • specify granted initial values (`InitialTime, InitialTotalVolume, InitialInputVolume, InitialOutputVolume, InitialServiceSpecific`)
	  • specify date/time for quota activation, expiration, or duration (`ActivationDateTime, ExpirationDateTime, Duration`)
	
	To display pool dynamic quota:
	• *Display a pool quota or pool dynamic quota*
		SDM Subscriber Provisioning User Guide
		• SPR pool provisioning templates (XML)
		• SPR pool provisioning templates (XML-REST)

	To map service indications (WebCI): • *Configuring SPR Service Indications*	*SDM System Configuration User Guide*

REST-API update of multiple fields in single command

The SPR XML-REST provisioning interface supports the update of up to three fields in a single command for subscriber or pool profile data. The update operation uses the PUT command and triggers only a single Sh notification per update request.

All fields (including multi-value fields) of subscriber or pool profiles that can currently be modified in a single-field request can also be modified in a multiple-fields request.

All fields are updated at once in the database and all values must be valid for the update to complete. The system returns an error message for an invalid value.

For more information about the Set Field Value operation, its syntax, and provisioning examples, refer to *XML-REST operations overview* and *Set Field Value operation* in the *Subscriber Provisioning Reference Manual*.

Chapter 4

High availability

Topics:

This chapter describes how the SDM system provides high availability.

High availability

High availability is the ability to tolerate certain faults during operation of the system and continue to provide service. A highly available system employs various techniques to detect faults and manage failures so that overall service is not affected. Where possible, the system also automatically attempts to recover failed components.

In the SDM, a combination of hardware and software functionality is used to provide high availability of the system services. Two overall techniques are used:

- The system's fault detection capabilities are used to identify failures in a timely manner.
- Failure toleration and recovery allows the system to manage failures and deploy redundant resources to maintain service. Where possible, automatic recovery of failed components is attempted.

Failure toleration and recovery

Hot swap hardware

Hot swap allows defective hardware units to be replaced without requiring the system to be powered down.

Clustering:

At the shelf level, individual node boards are organized into two cluster groups:

- Active/Standby (1+1)
- N-Active (N+0)

Only the slots provisioned with the System Controller identity run in an active/standby model. An instance of the CoreSystemController Service is found on a pair of nodes. A single instance of the CoreSystemController Service running on two blades identify a redundancy group with a 1+1 redundancy policy: when one instance of the CoreSystemController Service in the group fails, the other instance of the CoreSystemController Service automatically takes over and continues providing service.

For each active instance of the CoreSystemController Service there is a corresponding standby instance of the service.

However, the FrontEnd identity runs in a N-Active model. This means that an instance of the CoreServiceNode and of the User Service is distributed on each blade. All these instances are active at all time and if a service goes down, the load and traffic is redistributed among the remaining service instances on the other blades.

Software Redundancy:

Redundancy of the software applications is accomplished via the node clustering. Applications running on the System Controller identity's active node has a corresponding peer on the standby node. As for

applications running on the FrontEnd identities, multiple instances exist on each blade and run in an active state.

Database replication:

Replicated database ensures that database integrity is maintained in the case the active database fails.

Checkpointing and stateful “hot” standby

Application between active node and standby node in a redundancy group exchange state information via state journaling (or check pointing).

A failure of the active node or of an application on the active node triggers an automatic switchover to the standby node. Because of state journaling, the standby node is able to continue providing service without loss of state.

Automatic start, stop and restart policies

Provides automated mechanism for recovering failed components by restarting the failed hardware or failed applications.

Fault detection

Error reporting

Applications generate an error when something has gone wrong during processing.

Hardware sensors

Monitor various environmental conditions (temperature, voltage) which may influence the correct functionality of the system.

Automatic switchover (protection switching)

A switchover only occurs for services running in a 1+1 mode (PureProtected protection mode), which means it only occurs for the System Controller service. A failure of a node board or a software application for the System Controller service will trigger an automatic switchover from the active node to the standby node. The transition is completely managed by the system, based on the redundancy information in the system model.

Manual switchover

The operator can issue a command to manually trigger a switchover from the active node to the standby node for the System Controller. This command should be used with caution.

Switchover service continuity

Applications make use of check pointing between the active node and the standby node to preserve state information during a switchover.

A switchover has the following impact:

- · Database replication ensures database integrity, so the standby database is always up-to-date. During provisioning, committed transactions are preserved, while uncommitted transactions are discarded.
    - · Standby System Controller node immediately takes over from the failed active node. Remote OAM&P connections (e.g. remote connection to the CLI) will be broken and needs to be reconnected.

  For HLR continuity during a switchover refer to *HLR Server*

  For SS7 continuity during a switchover refer to *SS7 Manager*

  SIP continuity during a switchover refer to *Global Schema*

  A switchover of the System Controller does not impact the User services (Hlr service and Hss service). If the active System Controller goes down, a switch over occurs to activate the standby System Controller. In the mean time, the User Service's instance that is on the same blade as the previous System Controller that went down will be unassigned until the standby System Controller becomes active. While the User Service instance is unassigned on that blade, the other User service instances take on the load without any problems.

Chapter 5

Fault management

Topics:

This chapter describes fault management, including SNMP and database backup and restore of the SDM OAM&P subsystem.

Fault management

The SDM system is built on a distributed architecture providing system reliability, scalability, and robustness. According to the OSI network management specifications, the SDM OAM&P subsystem provides the following key management functionalities: Fault Management, Configuration Management, Performance Management, and Security Management.

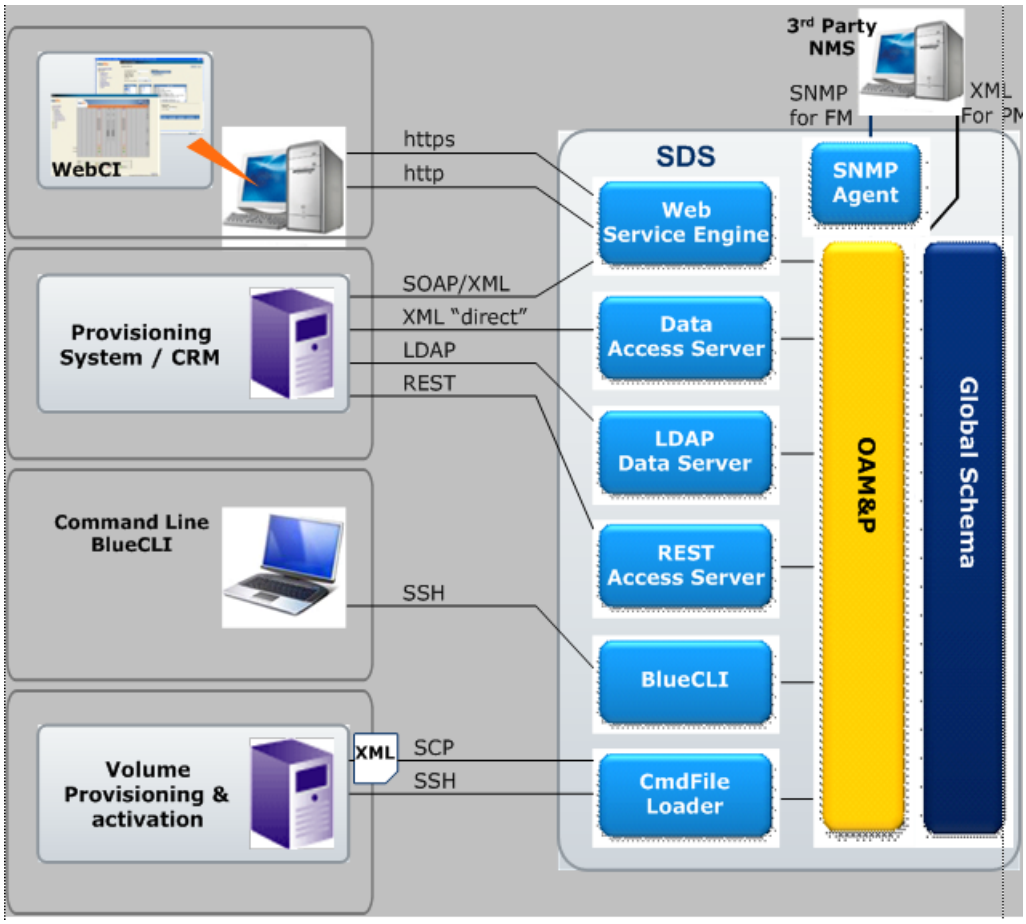


Figure 67: OAM&P interfaces

OAM&P

The OAM&P tools provide system access to the operator's system administrator, as well as system monitoring and control by communicating with the platform and applications. OAM&P operations are handled by the standard SDM mechanism and provide the following functions:

- System provisioning, configuration, and monitoring
- Subscriber and service provisioning and management
- Performance measurements
- User account management

The SDM Fault management system will detect faults and report alarms for the following functional areas:

- Change in operation state of an application and slot
- System initiated action
- Operator initiated operation

System software monitoring and recovery

The System Manager monitors the overall system behavior and generates system alarms. A software watchdog process is running on each blade and monitors the applications. It will perform an automatic recovery if the application fails. The watchdog generates appropriate alarms during the recovery/restart sequence. If the automatic recovery for a Module and slot does not succeed, an alarm is generated to alert the operator that manual intervention is required.

System monitoring is provided through the CLI and the WebCI. All active alarms, cleared alarms, and event logs are tracked and can be viewed for troubleshooting.

Active alarms

Active alarms on the system can be viewed from the CLI and WebCI. From the WebCI, a great deal of flexibility is provided in viewing the alarms. Any alarm event can be viewed and sorted according to its Sequence Id number, Alarm Id number, Severity accompanied with its corresponding color, Description, Shelf Id, Slot Id, Set time (time when alarm occurred), Set Last time (last time the alarm occurred), SetBy, Alarm Count (the number of times the alarm was set), Acknowledge time, AckBy and there is a last option that permits the operator to acknowledge and clear individually some alarms. In addition, the WebCI Alarm screen is dynamically updated.

Historical Alarms

The History Alarm list provides a chronological listing of all the alarms that have been set (created) as well as those that have been cleared on the system. Alarm events that have been set as well as cleared can be viewed and sorted in the WebCI's History Alarm window according to its Sequence Id number, alarm Id number, severity accompanied with its corresponding color, shelf Id number, slot Id number, alarm Set/Clear time, SetBy, ClearBy, alarm set last time, acknowledge time, AckBy and whether the alarm has been set/cleared. The alarms are listed in the order they occurred with the most recent at the top. Acknowledgement of an alarm and the user that acknowledged it is also logged in the History alarms. The History Alarm can be viewed from either the CLI or WebCI.

Logs/Events

Log messages are generated whenever an action or event occurs on the system. Logs provide operators with an additional level of information which allows them to verify correct operation of the SDM. Log files can be viewed from the CLI. System log messages are displayed in real time and reflect system activity as it occurs. The log files are generated for the current day and stored in a directory. Log files are rotated every night at 0:00 hours and are kept for a period of seven days

SNMP

The Subscriber Data Management supports SNMP (Simple Network Management Protocol) to provide Network Management Systems with real time alarm monitoring.

The SNMP implementation consists of a SNMP agent that interacts with the OAM&P Manager and the Network Management (NM) System. The agent interfaces with the OAM&P Manager to receive notifications whenever a change occurs on the system. The notifications are then mapped into Tekelec proprietary MIB OIDs (Object Identifiers) and sent to an external NM using SNMP traps.

The Tekelec SNMP implementation supports the following SNMP requests:

Request	Description
GET	The manager requests the values from one or more MIB variables
SET	The manager changes one of the MIB variables.
TRAP	Send an unsolicited notification to inform the Network Manager of a significant event.
WALK	An SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information

Traps

There are seven generic trap messages that are supported for Alarms Raised (4), Acknowledge (1), Clear (1), and Synchronization (1):

- Critical Alarm
- Major Alarm
- Minor Alarm
- Warning Alarm
- Alarm Acknowledgement
- Alarm Cleared
- Synchronization Request

These traps notify the Network Manager of any alarm conditions that are raised, acknowledged or cleared on the Tekelec network element.

The SNMP agent also supports a heartbeat notification trap that is sent to the NM System at heartbeat intervals that can be defined by the Network Operator by configuring the SnmpHeartbeatTime parameter of the Shelf entity. This heartbeat notification can be enabled/disabled by the Network Operator by configuring the SnmpHeartbeatEnabled parameter of the Shelf entity.

For more details on the Shelf entity and on the SNMP parameters, refer to the "Shelf" and "SNMP Trap Configuration" sections of the SDM System Configuration-Reference Manual and for instructions on how to display/edit the SNMP configuration from the WebCI, refer to the "Viewing/Editing SNMP configuration" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

MIBs

The Tekelec proprietary MIB (Management Information Base) is designed for alarm notification purposes. It is separated into two MIBs: SMI root and System MIB. Refer to the "SNMP" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual* for additional details on these MIBs.

Versions

The Tekelec software supports the following versions of SNMP:

- SNMPv2c (2nd release of SNMP described in RFC 1902). It provides additions to data types, counter size, and protocol operations. It is recommended to use SNMP V2C for SNMP GETS and TRAPS. It is not recommended to use SNMP V2C with SNMP SET.
- SNMPv3 (most recent version of SNMP described in RFC 2271-2275). It adds security and remote configuration capabilities to the previous versions. It is recommended to use SNMP V3 with SNMP SET.
- SNMPv1 (initial version of SNMP described in RFC 1157) can be used for SNMP SETS and TRAPS. However, it is not recommended.

Synchronization

In order to ensure the Network Manager is maintained with the same alarm information as the Tekelec SDM, a synchronization request can be issued. Synchronization can be performed under the following situations:

- Network Manager start up.
- Tekelec SNMP agent issues a Synchronization Request
- Periodically:
  - Programmed automatically at regular intervals
  - Manually

Versions

The Tekelec software supports the following versions of SNMP:

- SNMPv2c (2nd release of SNMP described in RFC 1902). It provides additions to data types, counter size, and protocol operations. It is recommended to use SNMP V2C for SNMP GETS and TRAPS. It is not recommended to use SNMP V2C with SNMP SET.
- SNMPv3 (most recent version of SNMP described in RFC 2271-2275). It adds security and remote configuration capabilities to the previous versions. It is recommended to use SNMP V3 with SNMP SET.
- SNMPv1 (initial version of SNMP described in RFC 1157) can be used for SNMP SETS and TRAPS. However, it is not recommended.

Synchronization

In order to ensure the Network Manager is maintained with the same alarm information as the Tekelec SDM, a synchronization request can be issued. Synchronization can be performed under the following situations:

- Network Manager start up.
- Tekelec SNMP agent issues a Synchronization Request
- Periodically:

Database backup and restore

Backup

The operator can perform the backup operation to create a consistent snapshot of the database while the system is active. The backup covers the subscriber's profile data, system configuration, and alarm history. The resulting backup files are stored onto the active System Controller (SC).

It is possible to back up database segments:

- Subscriber profile data.
- Alarms
- OamConfiguration.
- HlrConfiguration
- HssConfiguration

The operator can also activate an automatic backup for subscriber profile data and optionally configuration data. To do this, the operator must set the DatabaseBackupSchedule for an automatic backup, by defining the hour, minutes, BackupDirectory, FileRotation and the IncludeConfiguration option. Once the DatabaseBackupSchedule is set, the automatic backup needs to be activated for the backup to take place (refer to *Automatic backup* for more details on the automatic backup feature).

The manual and automatic backups can both be launched via the CLI and WebCI. For the step-by-step procedures, please refer to the "Creating a backup of the system" section in the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Restore

The Restore operation can be used to rebuild a damaged or corrupted database. It will use the database file that was copied from the Backup operation. The restore operation will restore the full database information onto the active System Controller.

Restore operations can be done from CLI and WebCI. For the step-by-step procedures, please refer to the "Restoring the system from a backup" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

SDM Support for NetBackup

Description

Subscriber Data Management supports the Symantec NetBackup utility on SDM clients when installed with an existing customer NetBackup server. Installation and configuration of NetBackup on SDM is normally done in collaboration with the Tekelec field installers and the Network Operator NetBackup administrators.

The NetBackup utility manages backups, restores, and disaster recovery of remote systems and is often used in large network operations with centralized data backup infrastructures.

A NetBackup configuration eliminates or reduces the need for backups using ISO images generated by native Tekelec Platform Distribution (TPD) backup functions and the associated optical media handling. Furthermore, this configuration places backup policies entirely under the control of the NetBackup server, which contains the configuration of the files and directories to be archived, any archival policies, and backup schedules.

Hardware Requirements

The NetBackup utility can be configured on a standard SDM hardware configuration (c-Class, DL360,or PP-5160). However, this design implies that network bandwidth for SDM applications may be adversely affected while backups are in progress. Instead, Tekelec recommends to plan for dedicated network ports for NetBackup traffic.

For an HP c-Class environment with dedicated backup network connections, this feature requires BL460c G6 blades with at least one TPD-supported mezzanine module in each blade requiring the backup connection. The feature requires two additional TPD-supported c-Class enclosure switches to support additional network connections.

For HP rackmount environments, the supported configuration consists of DL360 servers with two onboard gigabit Ethernet ports and a quad gigabit Ethernet card (for a total of six gigabit Ethernet ports). If the configuration uses a dedicated backup network, one of these six gigabit ports must be reserved to NetBackup traffic on every SDM server that will be a NetBackup client.

This feature can also be implemented on a PP-5160 with at least four gigabit Ethernet ports.

Software Requirements, Installation, and Testing

The Symantec NetBackup client software licenses are provided by the customer. The software is installed on the SDM on top of the TPD software. TPD supports Symantec NetBackup versions 7.0 or 7.1 for 64-bit servers. The Network Operator selects the version during the installation.

The Network Operator uses the TPD platcfg utility to install the client software on the SDM application server. During software installation, the Network Operator enables the application server to receive the client software and configures the IP address and host name of the NetBackup server in file `/etc/hosts` on the SDM hosts that will be NetBackup clients. The NetBackup server then transfers the client software to the application server. On the application server, the network operator installs the client software, configures it to support the feature, validates it, and disconnects the transfer.

The Network Operator can test the connectivity from the NetBackup server by typing test commands, for example, `bpclntcmd`. The network operator can also test backups manually by initiating them through the NetBackup server; or through the NetBackup client, if client-requested manual backups are permitted in the server-controlled backup policy. Once at least one backup is taken of files on a NetBackup client, the network operator should test restoring arbitrary data files from the client or the server.

Backup and Restore Processes

Backups use a TCP/IP network. Depending on the chosen network hardware and cabling configuration, backup activity may occur on a network shared with user traffic or OAM, or on a network dedicated to backups. Data restores during a disaster recovery will also be carried out over this network.

During the backup process, the NetBackup server scheduler sends a backup request to the client. The SDM application server performs the backup using standard backup procedures and transfers the

files to the NetBackup server for storage. The backup will include SDM directories where the system and server backup files are contained and the SDM host name and IP address. Backups should be scheduled during periods of lower system activity.

For a restore, the NetBackup server transfers the files to the appropriate directories on the SDM application server, upon which standard SDM utilities complete the restore operation.

Note: The NetBackup Bare Metal Restore (BMR) functionality is not supported. In case of a total data loss on a TPD-SDM processor, the recommended restore procedures include re-installing SDM and the correct NetBackup client on the affected CPU, and then using NetBackup to restore the appropriate data files.

Network Configurations

The basic network configuration consists of the customer NetBackup server and one or more Tekelec SDM application servers (NetBackup clients).

The SDM application servers, in either a c-Class or rackmount configuration, support networks with an external management interface (XMI) or with dedicated uplinks for NetBackup operations. The following configurations show how the SDM can be integrated in a NetBackup network. All configurations can support Ethernet jumbo frames.

In *Figure 68: SDM rackmount configuration using XMI for NetBackup*, NetBackup traffic flows over (and shares bandwidth with) the same network connections that are used for OAM and remote database replication.

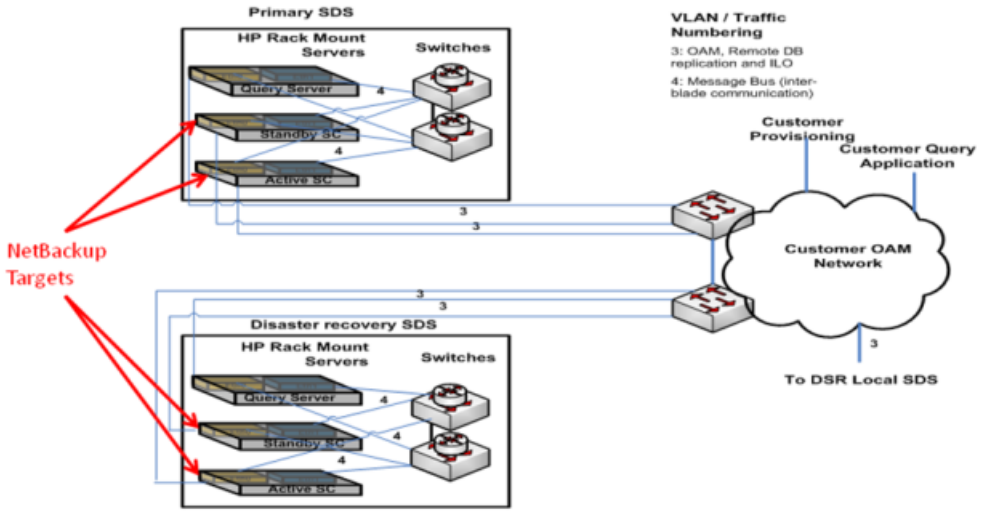


Figure 68: SDM rackmount configuration using XMI for NetBackup

In *Figure 69: SDM C-Class configuration using XMI for NetBackup*, NetBackup traffic flows over the same aggregation/enclosure switch paths as OAM and signaling traffic.

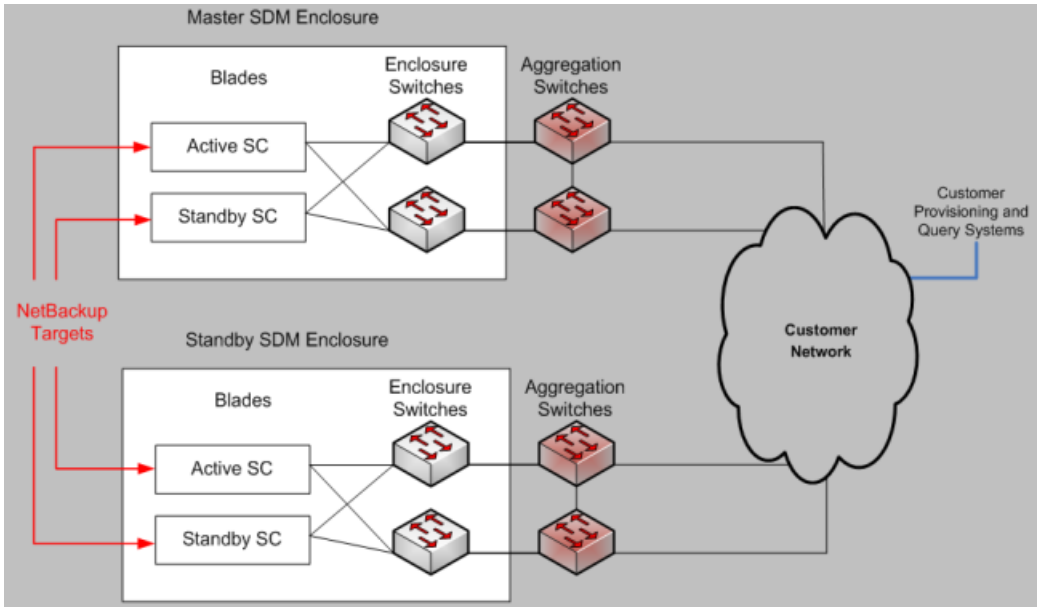


Figure 69: SDM C-Class configuration using XMI for NetBackup

The SDM DL360 configuration in *Figure 70: SDM rackmount configuration using dedicated uplink for NetBackup* requires a dedicated backup network. At least one network port must be dedicated to the backup connection on each SDM DL360 server. This configuration also requires a TPD-supported quad Ethernet card to be installed.

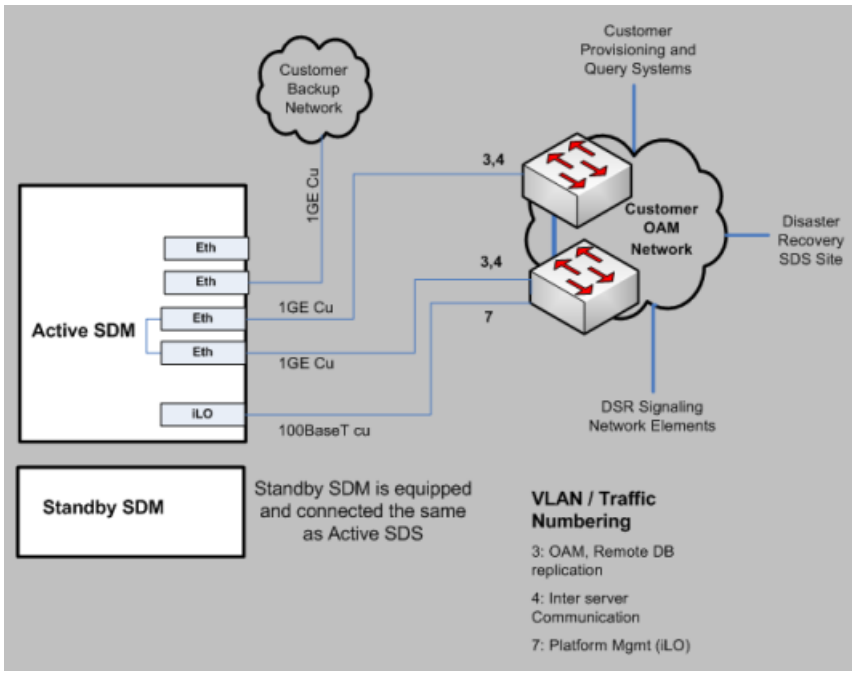


Figure 70: SDM rackmount configuration using dedicated uplink for NetBackup

The configuration in *Figure 71: SDM C-Class configuration using dedicated uplink for NetBackup* requires a dedicated backup network.

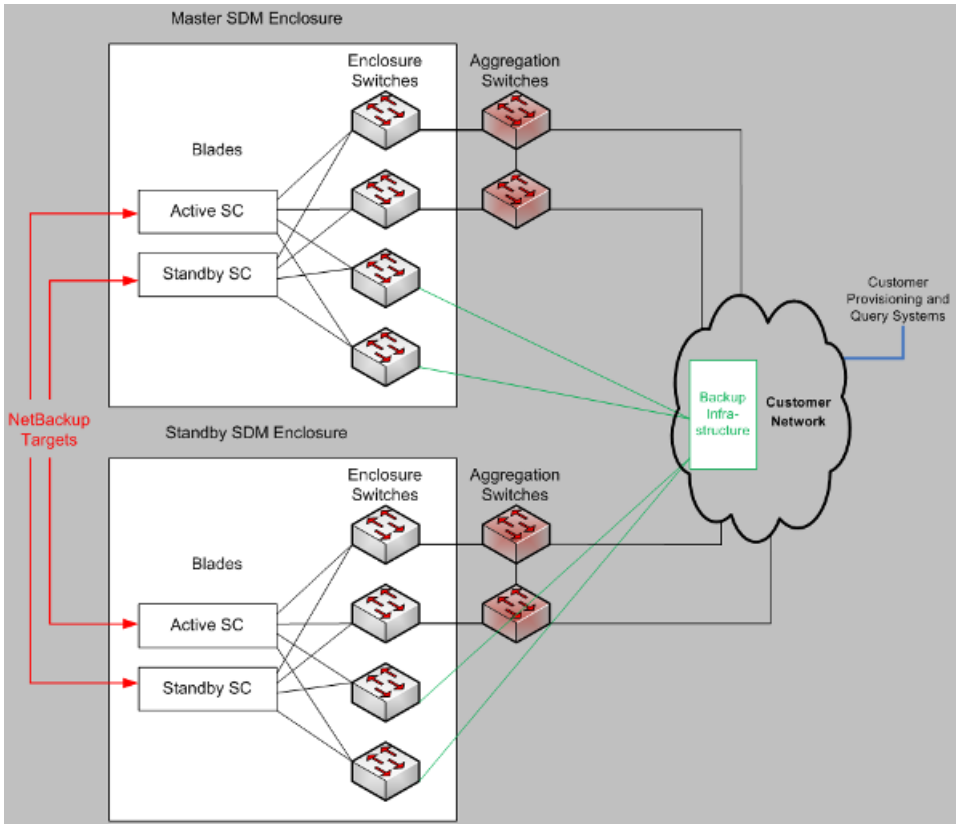


Figure 71: SDM C-Class configuration using dedicated uplink for NetBackup

Chapter 6

Configuration management

Topics:

The configuration management software provides features to

- list the identity, the type, and parameters of a configuration
- define default values
- modify operating characteristics

System provisioning and configuration management is provided via the CLI and WebCI interfaces.

HLR and SS7 Configuration

The installation and configuration of the SDM is performed by Tekelec field engineers prior to delivery. Configuration includes the setup for HLR and SS7. If any changes are required to the system configuration, please contact your Tekelec technical representative.

The HLR Global Provisioning can be used to display the configuration parameters for:

- The Authentication algorithms
- The Public Land Mobile Network
- The Camel GSM Service Control Functionality
- The Operator Controlled PLMN/IMSI selection feature
- The CSI Suppression feature
- The Bearer Capabilities
- The MAP Policing feature
- The SMS Redirect feature
- The Mobile Number Portability (MNP)
- The Subscriber Signaling Router (SSR)
- Enhanced Control of SCCP Routing Parameters
- XML Notifications for UL, UL-GPRS, SAI, Ready SM , Purge MS and CL

These parameters can be viewed through the CLI and WebCI.

- The SS7 configuration includes:
  - Physical and Data Link Level Parameters (MTP1, MTP2/SAAL) as well as Network Parameters (MTP3, SCCP, ISUP, TCAP)
- SS7 configuration parameters are viewable from the CLI and WebCI.
- Some SS7 modifications can be performed through the CLI and WebCI without necessary restart.

Sip configuration

The configuration of the Tekelec ngHLR for the SIP functionality is done prior to starting the SDM system and includes the main SIP configuration, the Registrar configuration, Security configuration, Redirect Server configuration and GSM Registration Agent (SIP User Agent) configuration. Once started, Sip Server configuration parameters are not modifiable. Sip configuration parameters are described in greater detail in the "SIP entities" section of the *SDM System Configuration - Reference Manual*.

HSS/AAA configuration

The configuration of the IMS-HSS in the SDM is performed by Tekelec field engineers prior to delivery. Configuration includes the setup for IMS-HSS, LTE-HSS, SLF, ENUM, AAA (if needed). If any changes are required to the system configuration, Tekelec technical representative.

You can view and provision the parameters for:

- HSS configuration
- HSS AuC
- HSS Subscription
- LTEHSS configuration
- SLF configuration
- Redirect Host Mapping provisioning
- ENUM configuration
- ENUM Subscription
- AAA configuration
- AAA Provisioning Configuration (AAA Dynamic IPAddress Allocation)
- AAA Subscription

In the SDM, you can configure and provision the IMS-HSS, the HSS subscriptions, if needed, the SLF and Redirect Host Mapping, the AAA and AAA Subscriptions as well as ENUM Users, all through CLI and the WebCI

Chapter 7

Subscriber provisioning

Topics:

Subscriber provisioning can be done via the CLI and WebCI interfaces. New subscriber profiles can be added. Existing subscribers can be modified, deleted, or displayed.

Services associated with each subscriber can also be added, modified, deleted, or displayed.

XML Provisioning

The Tekelec OAM&P Manager supports external provisioning and configuration management. This can be done from the OAM&P manager which processes Extensible Markup Language (XML) requests to provision subscriber profiles. The system can process requests through two modes: direct mode and batch mode.

- **Direct mode**

  (through a SOAP interface) will accept XML requests and be processed immediately by the SDM system
- **Batch mode** (through the CmdFileLoader tool) will accept a file containing XML requests and then process the requests. This mode is useful when processing many subscribers at the same time.

The OAM&P Manager supports requests generated in XML as defined by the World Wide Web Consortium (W3C).

The OAM&P Manager supports the following types of XML Requests

- **Insert**

  (add new entities and attributes)
- **Update**

  (modify entities, attributes, and attribute values)
- **Delete**

  (delete existing entities and attributes)
- **Select**

  (view and select a specific instance of an entity)
- **Operation**

  (invokes an operation on an entity)

The SDM also supports another way of provisioning subscribers by using templates. Templates can be defined using the XML language and loaded into the system's database through the Command Template Loader tool. These templates can then be referred to in the XML Request Templates created to provision subscribers.

Command File Loader

The Command File Loader is a tool designed for bulk provisioning. It is capable of reading a file of XML commands and submitting it for processing.

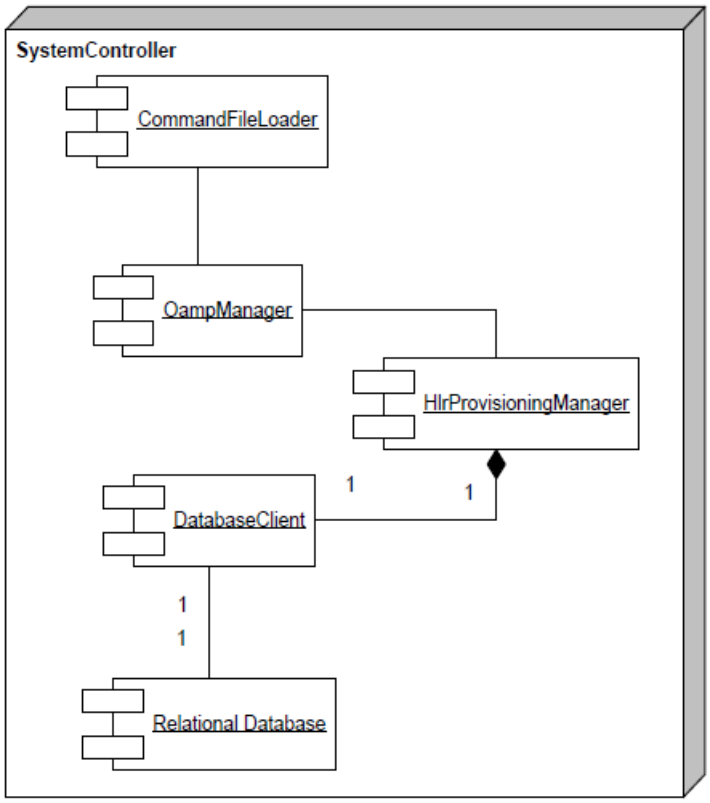


Figure 72: CommandFileLoader component diagram

The high availability framework ensures that the request is applied against the active database. Initially, all requests from external processes such as the CommandFileLoader are directed to the OAM&P Manager. The OAM&P Manager determines the module capable of processing the request. In the case of bulk provisioning, the requests are dispatched to the HlrProvisioning Manager or the HssProvisioning Manager. The HlrProvisioning Manager or the HssProvisioning Manager validates the requests and applies them against the database using the database client interface.

Command Template Loader

The Command Template Loader tool is designed for loading template files (in XML language) into the database in order to support subscriber provisioning with templates. The SDM provides an XML interfaces for creating and using templates in the provisioning commands. The support of templates in the system's database simplifies the provisioning interface by allowing to hide a lot of complexity in Templates

A Template file is made up of two entities: Template and Template Requests. The Template and associated Template Requests have to be defined in the database of the SDM. Once a Template file is defined, the tool used to load that template is called the CmdTemplateLoader. Please refer to the *SDM Subscriber Provisioning - Reference Manual* for more information and an example of a defined template and refer to the SDM Subscriber Provisioning - User Guide for information on how to load the template

with the Command Template Loader tool and for an example of a Request Template, which is a file made of "provisioning commands" that use the templates stored in the database to provision subscribers.

Request Templates are XML Requests of type "Template", and have to be created by the operator to use provisioning Templates. These templates are then used to create all requests necessary for provisioning all fields in all tables.

In a Request Template, only the attributes and values that correspond to variable fields need to be specified. The other attributes are statically defined in the templates stored in the database of the SDM. The Template Id of the Template to be used needs to be specified as well as Request template instructions (i.e., tpi), which provides a specific attribute and value pair that are used to override the default attribute values found in Template Requests associated with the specified Template

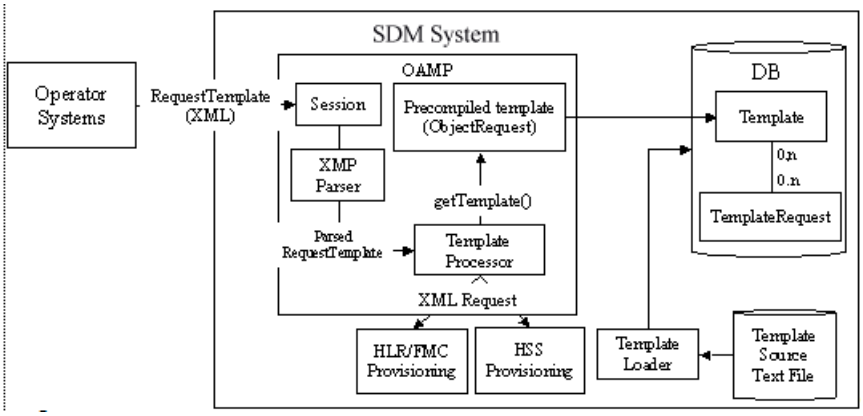


Figure 73: CommandTemplateLoader component diagram

As depicted in the figure above, the Command Template Loader tool has the role of loading Template files in XML language onto the database, where they will be stored.

The two Template and Template Request entities are stored in the database and are defined as follows:

- · **Template Request:** Each instance of this entity contains a single XML request, which represents a database operation using attributes with "over writable" /default values. A template request may be associated to several Templates. A template request doesn't contain any information on attribute constraint. The constraint definitions are done at the Template level. Template Request definitions are stored in the database in the original XML request format. Please refer to the *SDM Subscriber Provisioning - Reference Manual* for examples on the original XML request format.
- · **Template:** It mainly contains an association of several Template Requests. It also contains constraints for Template attributes that can be overwritten. These constraints specify the list of attributes which:
  - Have to be modified (MUST be found in a provisioning request)
  - Can be modified
  - Cannot be modified

The Template Requests are provisioned in the database using the Command Template Loader tool with an input of a XML file.

License Management

The License Management feature is designed to support HLR, SIP, IMS-HSS, SLF, SPR and AAA licenses. Take note that at startup, no license is loaded. The necessary licenses must be purchased by the operator as needed and loaded by the Tekelec *Customer Care Center*.

The SDM License Manager tracks the following:

- The number of active and total HLR subscribers registered on the system.
- The total number of SIP subscribers provisioned in the Tekelec ngHLR (i.e number of Address Of Records) and the number of SIP active subscribers (i.e., number of Registration Bindings)
- The total number of IMS-HSS subscribers provisioned for the IMS-HSS. A provisioned IMS-HSS subscriber corresponds to a link between a Private Identity and a Public Identity, which is an entry in the HssPrivatePublicLink entity
- The total number of SLF subscribers provisioned for the SLF. A provisioned SLF subscriber corresponds to a link between a PublicIdentity and a IMS-HSS Host Name hosting the PublicIdentity, which is an entry in the HssSlfPublic2HssName entity
- The total number of AAA subscribers provisioned for the AAA. A provisioned AAA subscriber corresponds to the couple AAA UserId+Authentication Method, which is an entry in the AAAUserId entity (identified by the AAAUserName)
- The total number of SPR subscribers provisioned for the SPR.

The SDM License Manager takes into account HLR, SIP, IMS-HSS, SLF, SPR and AAA licenses. The SDM allows or denies new subscribers to be provisioned based on the total number of HLR/SIP/IMS-HSS/SLF/AAA subscribers as defined in the licenses. Please note that while the system generates an alarm when the maximum number of SPR subscribers has been reached, it will still allow further SPR subscriber provisioning. When the alarm is raised and remains raised, we strongly advise you to contact Tekelec's sales team to purchase another SPR license with a higher value.

The number of active and total HLR/SIP subscribers registered can also be controlled by allowing the operator to provision thresholds. The SDM raises warning alarms when an operator defined threshold level has been reached for the number of HLR/SIP active subscribers or total subscribers. Critical alarms are also raised when the maximum number of HLR/SIP active or total subscribers, as defined in the license, has been reached. License logs are generated to indicate the number of active subscribers during each calendar month

In addition to defining the total number of IMS-HSS subscribers, the AAA license also defines the AAA RADIUS TPS limit. This allows the SDM to control the AAA traffic based on the maximum AAA RADIUS TPS that can be supported. If the TPS reaches the threshold defined by the configured AAA TPS license, the messages are silently discarded

It is important to note that in order to absorb burst of traffic with any impact, the IMS-HSS and AAA will accept the TPS License threshold to be reached during 60 seconds. If after 60sec. the traffic has not decreased under the allowed TPS license threshold, the IMS-HSS/AAA will begin to reject/discard incoming messages.

The SDM raises critical alarms when the maximum number of total IMS-HSS/SLF/AAA/SPR subscribers, as defined in the license, has been exceeded. It is important to note that all of these alarms remain active until the license is renewed.

Finally, through the CLI and WebCI, the operator can do the following regarding the system's License Management:

- View all current License values (HLR, SIP, IMS-HSS, SLF, AAA/SPR)
- View on a daily basis the number of HLR active subscribers with the license logs generated for each calendar month.
- Provision thresholds for both HLR/SIP active subscribers and total subscribers.

For more details on how to view the current License Management and monthly License logs, as well as on how to provision thresholds, refer to "Installing/Viewing the License" section of the *SDM Monitoring, Maintaining, and Troubleshooting - User Guide*.

Chapter 8

Performance management

Topics:

Counters allow the operator to manage system performance.

Counters

Counters allow the operator to manage system performance:

- **Traffic data counters.**

  Traffic data can be gathered from the system in order to allow an operator to analyze the system behavior. The role of the counters in the SDM is to report the number of MAP, SIP, IMS-HSS/SLF and AAA messages that have been processed in a successful or unsuccessful way by the system during its runtime. This is very useful to help in knowing how an application service behaves among the other applications running on the network.

- **HLR Subscriber counters.**

  Twelve types of HLR-specific subscriber counters have been implemented to count HLR subscribers. This dynamically keeps track of the number of HLR subscribers on a SDM system. The WebCI displays these counters in the PMCounterValue window of the Oamp folder. Through this window, the operator can view each of the counter's count value reported after each 15 minute or 24 hour period for the current day

- **OS Resource counters.** These counters monitor the CPU load, process information, memory usage, disk I/O operations and IP network interface utilization for all of the processes running on each blade. The current value of each of these counters can be viewed from the WebCI's PMCounterValue window. Refer to the SDM Performance Measurements for step-by-step instructions on how to view the current counter value from the WebCI.

For some of these counters, a major and minor threshold, or simply one single threshold, are pre-defined in the system. The thresholds indicate to the system when to generate and clear an alarm. Refer to the SDM Performance Measurements for step-by-step instructions on how to edit these thresholds from the WebCI.

All these counters can be viewed from the CLI:

- In the file dumped every 30mins by the PerfCollector tools in /blue/var/pm
- In the file dumped every day by the system itself in /blue/var/pm which displays the result in an easy human readable form.

For step-by-step procedures on how to view the Performance Measurements through the CLI, refer to the *SDM Performance Measurements* document.

Chapter 9

Security management

Topics:

This chapter describes the various levels of security the SDM provides to prevent unauthorized access to the system.

SSH

Remote computer connections are done using SSH (Secure SHell). SSH is a tool for secure remote login over insecure networks. It provides an encrypted terminal session with strong authentication of both the server and client. SSH to a blade requires a login session.

HTTPS

The Web-based Graphical User Interface (WebCI) uses the **https** URI scheme to assure a secure HTTP connection. Using the HTTPS protocol (port 8443) to access a secure web server provides authentication and encrypted communication. Before entering the WebCI, each user must enter their UserName and UserPasswd. The SDM also supports the possibility for the operator to disable the Web Service Security in order to access the WebCI through the HTTP protocol (port 8080). The Web Service Security is a Service Option that can be disabled from the WebCI in the Service Management provisioning window under the System application folder.

Authentication center

The Authentication Center (AuC) is used to provide authentication and radio link privacy to users on the GSM network. The Authentication Center supports XOR and Milenage algorithms. Optional support can be provided for COMP128, COMP128-2, and COMP128-3.

IMS-HSS Authentication center

The IMS-HSS Authentication Center is used to provide authentication to users on the IMS network. The Authentication Schemas supported are the Digest AKA V1-MD5, the Digest-MD5, the HTTP_DIGEST_MD5 and finally NASS-Bundled. The ETSI TISPAN defines the algorithms for the HTTP_DIGEST_MD5 and NASS-Bundled Schemas. In the IMS-HSS AuC, specific algorithms can be provisioned for the supported Schemas.

User Security

Single Board Computer (SBC)

The Network Operators can take advantage of several interfaces offered by the SDM system to access the Single Board Computers: WebCI, SOAP, user application using XML, LDAP, CLI (using LINUX console), etc.

The User Security Management functionality is implemented in several of the system's processes in order to provide the login security (and not request content security) and control the user access privileges for:

- All the access interfaces: WebCI, SOAP, LDAP, CLI (using LINUX console), etc. The users that wish to access the SDM's interfaces must provide the following authentication information:
  - User name
  - Password
  - Application Id (automatically provided for the SDM system's applications: WebCI, CLI, etc.)
- The system's external applications that wish to receive notifications. This means that with the USM functionality, the Network Operator can control which user is allowed to request which type of notification from the SDM system. The applications that connect to the SDM system have to provide the authentication information, which includes:
  - User name
  - Password
  - Application name

Once the login is passed successfully, all the requests have to be checked against the user access privileges to ensure the right access of the user.

For more details on the XML authentication from an external node, refer to the 'Authentication Properties' sub-section of the "Subscriber Provisioning using XML Templates" section in the *SDM System Configuration - Reference Manual*.

Database

The database can be accessed for maintenance with the default username and password stored in the database itself.

At installation, the database is installed with a username and password by default that the administrator must change before starting the system for the first time. To do so, please refer to the step by step instructions given out in the "Creating and Managing user for the User Interfaces" section of the *SDM System Configuration - User Guide* .

External connections and requests logging

The SDM is equipped with a logging functionality managed by the User Security Management (USM) process that can log all/some external connections and requests. This functionality provides the capability to log the external connections to the system in the database either for investigating problems or for security verifications. It also allows to log the received requests in XML format.

By default, the connections are always logged and the requests are never logged. While the connections must always be logged, the logging of requests is configurable (either from the CLI or WebCI) by the Network Operator and can be turned on (activated) or off (deactivated) for different users and applications, by setting the Oamp UserApplicationMap entity's 'LogOption' parameter to the desired value. For details on the 'UserApplicationMap' entity and its parameters, refer to the "Notification

Security Management" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*. For instructions on how to provision the 'UserApplicationMap' entity, refer to the "Creating and Managing users/applications for the Notifications" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

By default, the connections are always logged and the requests are never logged. While the connections must always be logged, t he logging of requests is configurable (either from the CLI or WebCI) by the Network Operator and can be turned on (activated) or off (deactivated) for different users and applications, by setting the Oamp UserApplicationMap entity's 'LogOption' parameter to the desired value. For details on the 'UserApplicationMap' entity and its parameters, refer to the "Notification Security Management" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual* . For instructions on how to provision the 'UserApplicationMap' entity, refer to the "Creating and Managing users/applications for the Notifications" section of the *SDM Monitoring, Maintaining, Troubleshooting - User Guide*.

Every time a new connection is established to the SDM's XmlDataServer, an existing connection is terminated, or a failed attempt to connect is performed, an entry is added in the 'ExternalConnectionLog' entity, along with the following main information:

- The name of the user connecting
- The name of the application connecting
- The operation performed on the connection. A log is generated for the following operations:
  - When a connection is established using an external interface
  - When a connection is terminated by the client
  - Whenever an authentication failure occurred for a connection
  - When a connection is terminated by the server
  - The time of the operation

When the logging of requests is activated, depending on the logging option configured in the UserApplicationMap entity, allowed or denied requests coming from an interface are logged and are stored in the 'RequestLog' entity, along with the following main information:

- The connection in which the request has been received
- The request type
- The timestamp
- The request in XML format

An entry is added to the 'RequestLog' entity after the request has been processed, which means that the XML string stored contains not only the whole request but also the result of the execution.

Take note that in contrary to the connections, requests received from non-XML interfaces (LDAP, REST) are also logged, not just those received by the XmlDataServer.

In order to view these logs, simply display the 'ExternalConnectionLog' and/or the 'RequestLog' entity from the CLI. For details on these entities and their CLI navigation path, refer to the "External connections and requests logging" section of the *SDM Monitoring, Maintaining, Troubleshooting - Reference Manual*.

Chapter 10

Hardware description

Topics:

Tekelec utilizes industry standard off-the-shelf hardware combined with purpose-built software to provide a robust highly available system for operators around the world.

The Tekelec Subscriber Data Management (SDM) software solution is part of the EAGLE XG platform, which provides common hardware components so applications such as session management, policy management, and subscriber data management, policy management, and subscriber data manaement can be mixed and matched on server blades or rack servers in a central office or data center with AC or DC power.

This chapter describes the EAGLE XG hardware platform.

EAGLE XG platform overview

EAGLE XG is a high-capacity, low latency and highly reliable platform supporting a set of associated routing and database applications. The EAGLE XG platform offers:

- Field-proven, carrier-grade LINUX OS
- Support for mix of servers and blades
- Support for application co-mingling (for example: one application is deployable in the same footprint as other supported applications)
- Multi-threaded software that takes advantage of multi-core CPUs
- Regular security analysis relative to CERTS and industry bulletins
- High availability, automatic configuration, and upgrade/backout
- IPV4 support on OAM interfaces/IPV6 support on signaling links
- Deployment in Central Office or Data Center
- Proven global delivery and support capabilities

Figure 75: Subscriber Data Management (SDM) architecture provides an overview of the EAGLE XG platform showing the hardware platform and the EAGLE XG applications.

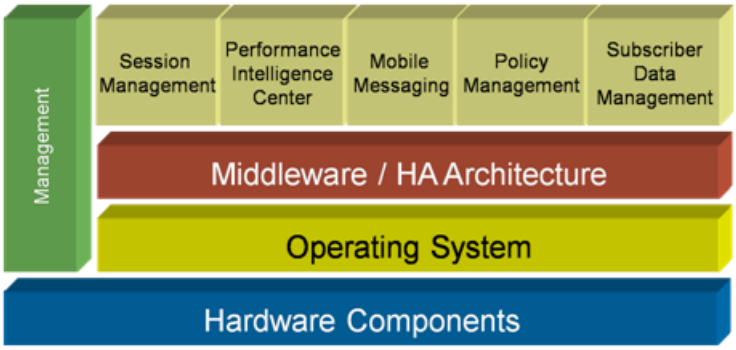


Figure 74: EAGLE XG platform architecture

The EAGLE XG platform allows for deployment in a carrier-grade Central Office or an enterprise-class Data Center and employs both blades and rackmount servers for the EAGLE XG applications.

Figure 75: Subscriber Data Management (SDM) architecture provides an overview of the SDM architecture with SDM applications and applicable hardware components.

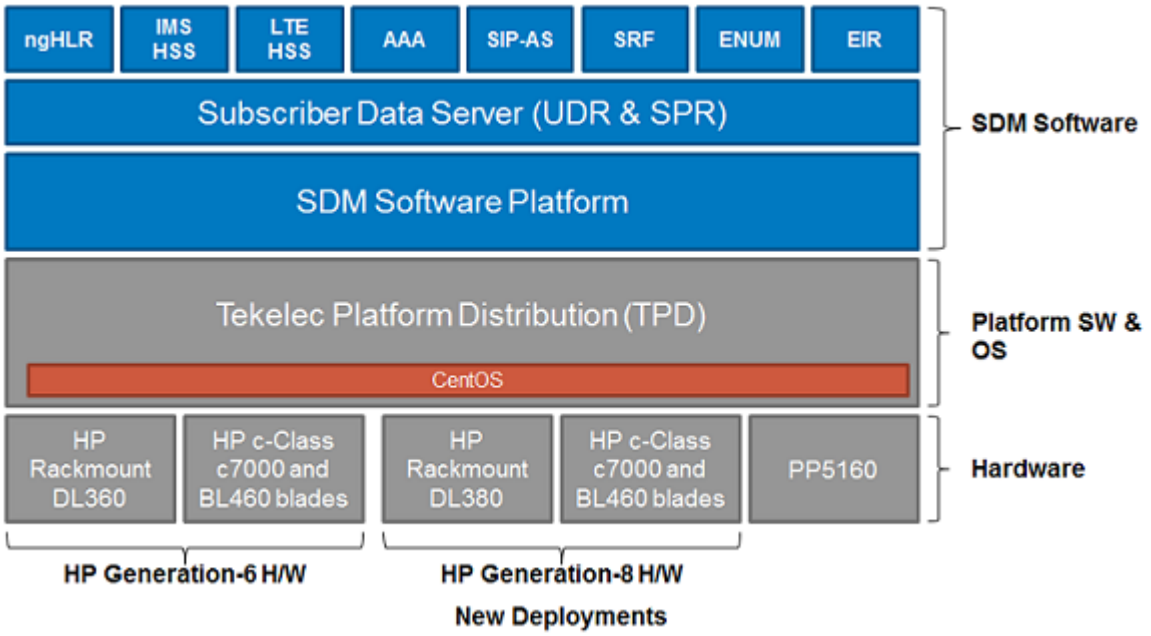


Figure 75: Subscriber Data Management (SDM) architecture

The HP c-Class 7000 platform is composed of up to 16 BL460c application servers and D2200sb storage blades.

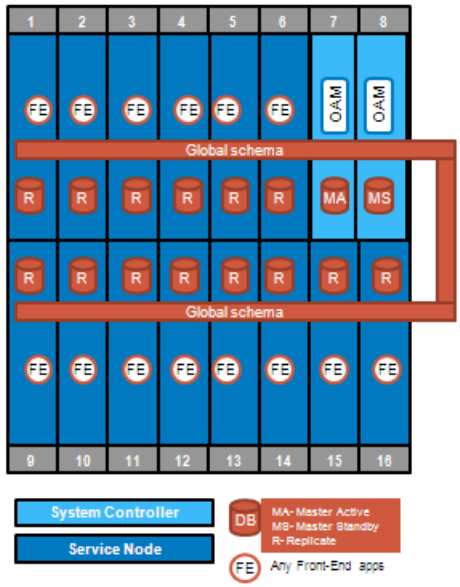


Figure 76: Example of HP c-Class architecture

A HP DL380 rackmount server hosts the platform, management, and configuration applications for the HP c-Class platform.

The rackmount server platform consists of two HP DL360 G6 or two DL380 Gen8 application servers. *Figure 77: Example of rackmount architecture* shows the rackmount server architecture with an application server pair.

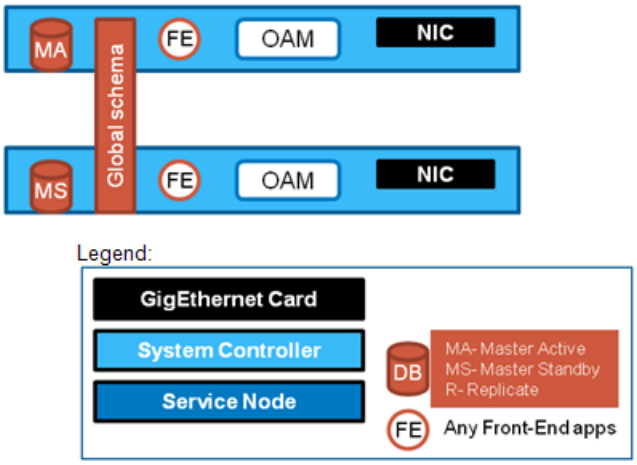


Figure 77: Example of rackmount architecture

All application servers can run any of the SDM applications. For example, SIP, IMS-HSS, SLF, LTE-HSS, AAA, WiMAX, ENUM, DNS, and EIR.

Tekelec supports the PP5160 platform for current customers using this platform with the Policy application.

The PP5160 is not described in this document. For details on the PP5160, refer to the *PP5160 Hardware Installation Guide* of your Policy Documentation set.

EAGLE XG hardware

EAGLE XG hardware is provided by third-party vendors and is assembled by Tekelec manufacturing. Customers may elect to purchase hardware directly from the same third party vendor used in Tekelec solutions according to specifications provided by Tekelec.

Table 33: EAGLE XG hardware vendors

Device	Vendor
Cabinet, power distribution panel, and cabling	HP, Telect, Noran Tel
c7000 enclosure	HP
Aggregation switches	Cisco
Enclosure switches	HP (Cisco)
Blade servers	HP
Rackmount servers	HP, Kontron
Enclosure power demarcation panel	Telect

The EAGLE XG hardware used for the Subscriber Data Management (SDM) application is available for AC and DC power. The hardware consists of the following cabinets and components depending on customer-specific configurations:

- Cabinets
  - HP Enterprise cabinet (AC)
  - Telect CoreMAX seismic cabinet (DC)
- Power distribution units (AC) or panels (DC)
  - HP AC PDU
  - Telect 100A 4-Position Demarcation DC PDP
  - Telect 100A Dual feed DC PDP
- Cisco 4948E/4948E-F aggregation switch
- HP c7000 enclosure with
  - Onboard Administrator
  - Cisco 3020 blade switch
  - HP BL460 G6/Gen8 blade server
  - D2200sb storage blade
- HP DL360 G6 rackmount server
- HP DL380 G6/Gen8 rackmount management/application server

For a brief description of each component, refer to the following sections.

For a detailed description of vendor components, refer to the *SDM Roadmap to Hardware Documentation* included in your SDM documentation set. This document provides links to the vendor sites and their downloadable product documentation.

Cabinet

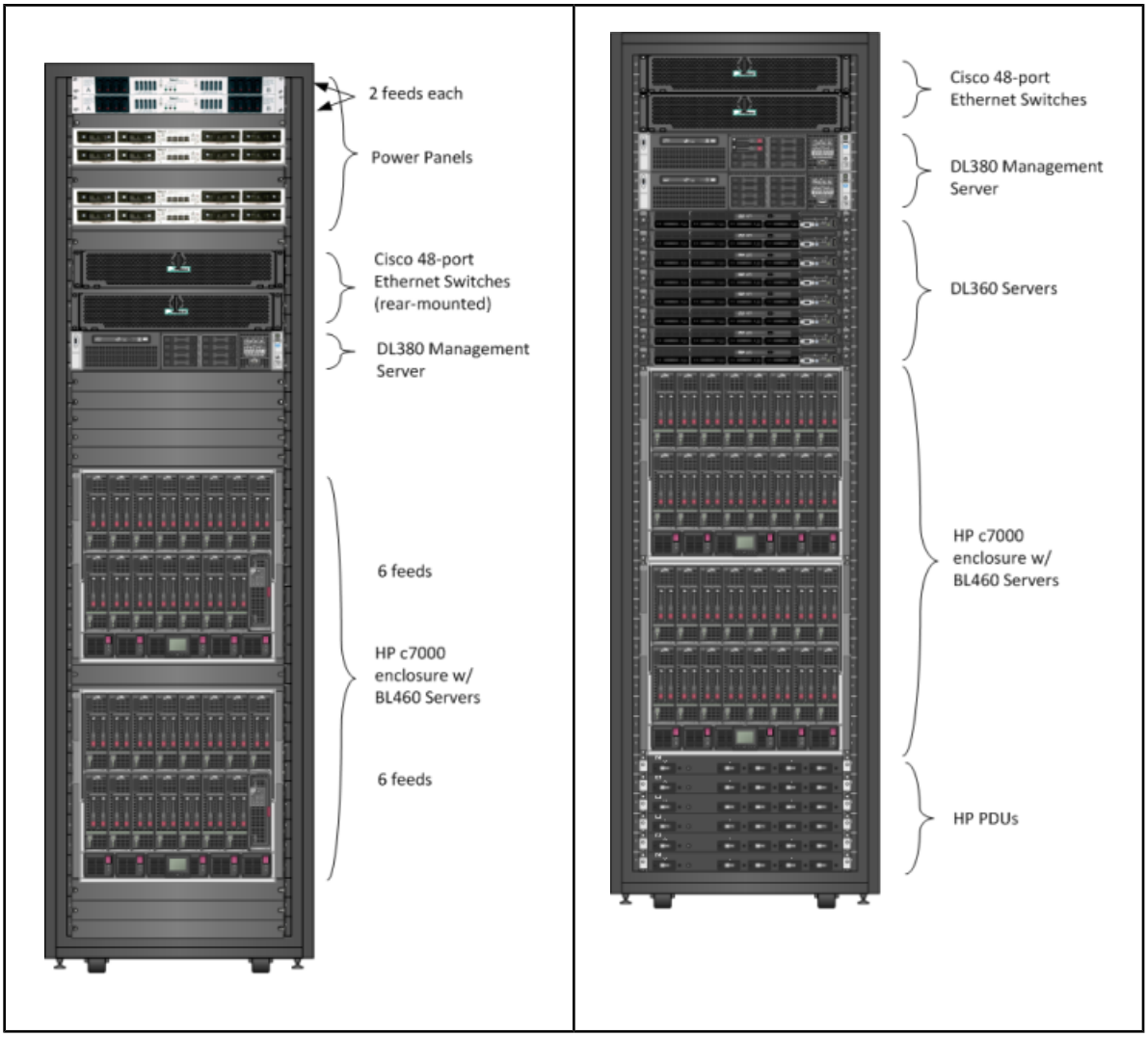
HP c-Class hardware powered by AC is mounted in the HP enterprise cabinet. HP c-Class hardware powered by DC for seismic applications is mounted in the Telect CoreMAX rack. Note that these cabinets are designed to allow for the equipment to be mounted prior to shipping. Equivalent cabinet configurations and/or suppliers may be substituted by Tekelec.

The DC cabinet can house up to two c7000 enclosures, aggregation switches, a management server, and power panels.

The AC cabinet can house up to three c7000 enclosures, aggregation switches, management server, and power panels

The figure shows examples of a DC c-Class and an AC co-mingled (c-Class and rackmount) cabinet configurations.

Figure 78: Example of DC (left) and AC (right) cabinet configurations



The table describes the power requirements for AC/DC frames:

Table 34: Minimum Power Requirement (AC/DC)

Power Measurement	DC	AC (North America & Japan)	AC (International)
Voltage	-48 VDC	200-240 VAC single phase	
Amperage	(8) 60A input feeds	(2) 50A input feeds	(2) 32A input feeds

Note: These power requirements are for minimally configured units. The power requirements for specific installations are determined by actual configuration and site survey information.

Telect 100A 4/4 Fuse Panel

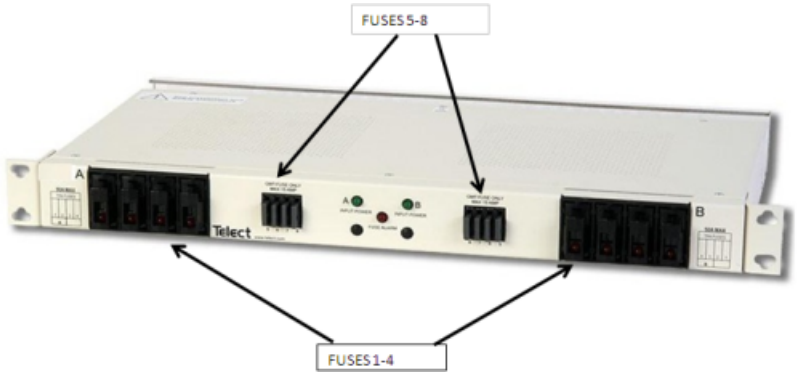


Figure 79: Telect 100A 4/4 fuse panel - front view

Figure 80: Telect 100A 4/4 fuse panel - rear view

High Current Demarcation Panel

The High Current Demarcation Panel is a 60A Telect DC power panel.

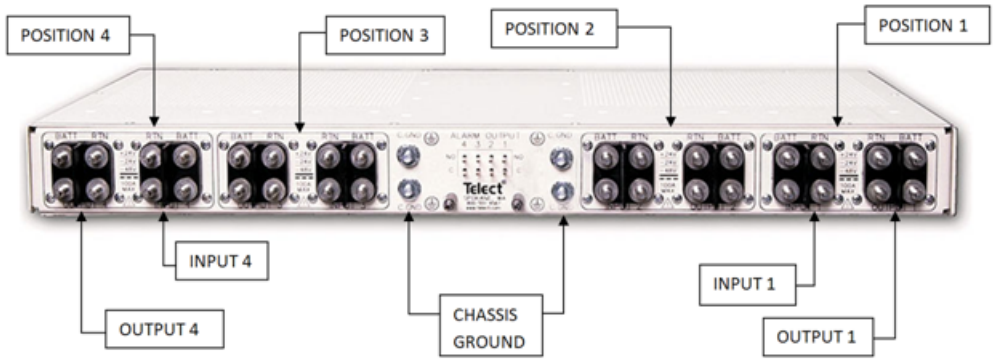


Figure 81: High Current Demarcation Panel - front and rear views

Aggregation Switch

The aggregation switches are optional and provide layer 2 or layer 3 demarcation between the SDM node and the network.

Aggregation switches are 1U high. The Cisco 4948E-F DC (Gen8) model requires a Panduit air duct, which increases the switch to a 2U unit.

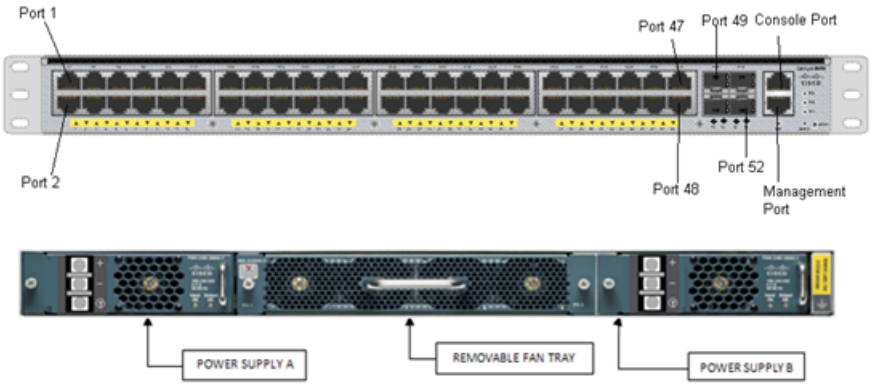


Figure 82: Cisco 4948E-F Aggregation Switch - front and rear views

HP DL360 G6 rackmount server

The HP DL360 G6 is a 1U rackmount server.

Each server can run any SDM application, for example, Tekelec ngHLR with Sigtran, SIP, IMS-HSS, SLF, LTE-HSS, AAA, WiMAX, ENUM, and DNS.

Figure 83: HP ProLiant DL360 G6 rackmount server

Table 35: HP DL360 G6 base features

Feature	Description
Processor	Up to two Hex-Core Intel Xeon 5500 Sequence
Memory	24 GB DDR3 RAM; options for up to 48GB DDR3 RAM
Internal Storage	2 Hot-plug SFF SAS/SATA drive bays 600GB/146GB Integrated Smart Array P400i controller with Flash-backed Write Cache
Networking	Two HP NC364T Dual Port Multifunction Gigabit Server Adapters (four ports total) with TCP/IP Offload Engine, including support for Accelerated iSCSI
Expansion Slots	Two PCI slots
Management	Integrated Lights Out 2 management
Form Factor	One rack-unit or 44.45 mm (1.75 inches)

HP DL380 G6 management server

The HP DL380G6 is a 2U rackmount server. It hosts the platform, management, and configuration applications, which provide configuration and management to the c-Class platform. In addition, the management server is used for FRU activities and for disaster recovery operations by providing Tekelec personnel with port access to server blades as required. The management server is deployed as a single server at each signaling NE site.

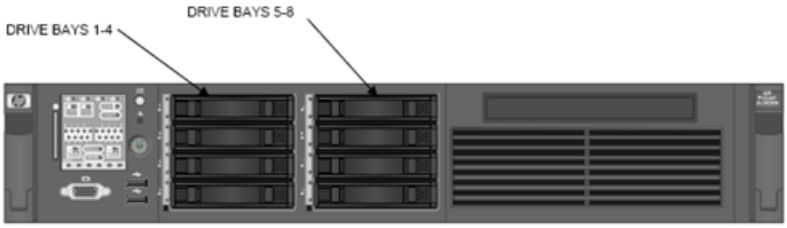


Figure 84: HP DL380 G6 rackmount server - front view

Table 36: HP DL380 G6 base features

Processor	Up to two Quad-Core Intel Xeon 5500 Sequence
Memory	24 GB DDR3 RAM; options for up to 192GB DDR3 RAM
Internal Storage	2 Hot-plug SFF SAS/SATA drive bays (600GB) Integrated Smart Array P400i controller with Flash-backed Write Cache

Networking	Two HP NC382i Dual Port Multifunction Gigabit Server Adapters (four ports total) with TCP/IP Offload Engine, including support for Accelerated iSCSI
Expansion Slots	Six PCI-Express slots
Management	Integrated Lights Out 2 management
Form Factor	Two rack-units or 88.9 mm (3.25 inches)

HP DL380 Gen8 rackmount server

The HP DL380 Gen8 is a 2U rackmount server. It can host EAGLE XG applications or be used as a management server.

As management server, the HP DL380 Gen8 hosts the platform, management, and configuration applications to support the c-Class platform. It can also be used for FRU activities and for disaster recovery operations by providing Tekelec personnel with port access to server blades as required. The management server can be deployed as single server or redundant pair at each signaling NE site.

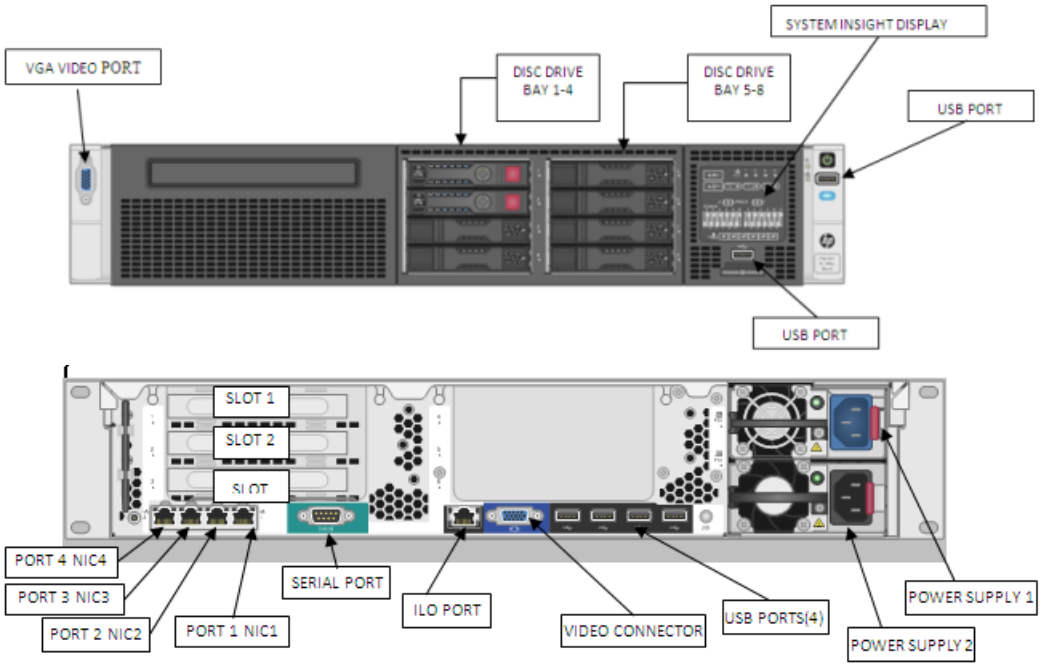


Figure 85: HP DL380 Gen8 rackmount servers - front and rear views

Table 37: HP DL380 Gen8 features

Processor	Two Octal-Core Intel Xeon E5-2600 Sequence
Memory	64GB or 128GB DDR3 RAM

Internal Storage	Hot-plug SFF SAS/SATA hard drive standard • 600GB drives for 64GB RAM configuration • 900GB for 128/192/256 GB RAM configuration Up to 14 additional SFF SAS hard drives as option
Networking	Four Multifunction Gigabit Server Adapters on-board Four additional multifunctional Gigabit Server Adapters via PCIe I/O card
Expansion Slots	Up to six PCI-Express slots
Management	Integrated Lights Out management

HP c7000 enclosure

This enclosure provides the power, cooling, and I/O infrastructure to support a modular server, interconnect and storage components.

The enclosure has the following features:

- 10U high
- Holds up to 16 half height servers and storage blades
- Pooled-power backplane
- Power input of single-phase, 3-phase AC, or -48V DC

The enclosure houses the HP-c-Class blade servers for OAM and message processing, enclosure switches, Onboard Administrator, and power modules.

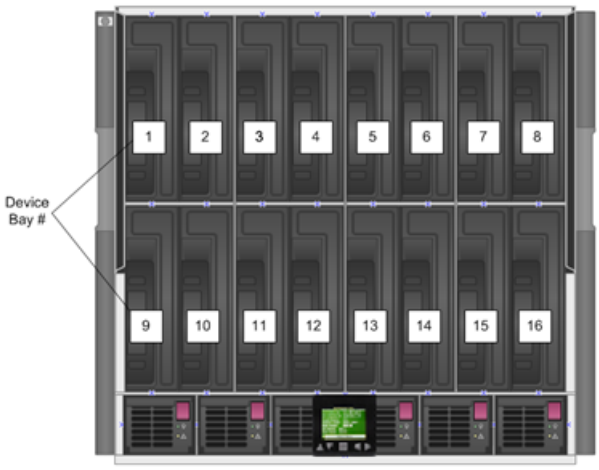


Figure 86: HP c7000 Enclosure Front View

Figure 87: HP c7000 Enclosure Rear View

HP BL460c G6 server blade

The HP BL460c G6 is a half-height server blade with two hard drives and installs in the HP c7000 enclosure.

Figure 88: HP BL460c G6 server blade

Table 38: BL460c G6 base features

Feature	Description
Processor	Up to two Quad-Core Intel Xeon 5500 Sequence or two Hex-Core Intel Xeon 5600 Sequence
Memory	24 GB DDR3 RAM; options for up to 192GB DDR3 RAM

Feature	Description
Internal Storage	2 Hot-plug SFF SAS/SATA drive bays 600GB Integrated Smart Array P400i controller with Flash-backed Write Cache
Networking	2 integrated Multifunction Gigabit Ethernet adapters Up to 4 additional ethernet adapters
Management	Integrated Lights Out 2 Standard Blade Edition
Form Factor	Half-height, single width c7000 blade

HP BL460c Gen8 server blade

The HP BL460c Gen8 is a half-height server blade with two hard drives and installs in the HP c7000 enclosure.

Figure 89: HP BL460c Gen8 server blade

Table 39: BL460c Gen8 features

Feature	Description
Processor	Two Octal-Core Intel Xeon E5-2600 Sequence
Memory	64GB, 128GB, 192GB, or 256GB DDR3 RAM
Internal Storage	2 Hot-plug SFF SAS/SATA drive bays • 600GB drives for 64GB RAM configuration • 900GB for 128/192/256 GB RAM configuration Integrated Smart Array controller with Flash-backed Write Cache

Feature	Description
Networking	2 integrated Multifunction Gigabit Ethernet adapters Up to 6 additional ethernet adapters
Management	Integrated Lights Out 2 Standard Blade Edition

HP D2200sb storage blade

The HP D2200sb storage blade is compliant with the HP ProLiant BL460c blade and is used for high-speed storage for back-end database performance. The blade provides the following:

- Up to 7.2 TB of raw internal SAS
- High-speed PCIe connection to adjacent BL460c blade
- Up to 12 600 GB SFF DSD hard disk drives
- Hot-plug SAS HDD

Figure 90: HP D2200sb storage blade

iSPAN5639L Interface Card

The 5639L (iSPAN5639L) interface card allows the HP BL460 blade server and the HP DL360 rackmount server to work on SS7/TDM networks.

The 5639L interface card provides the ngHLR with all necessary connections to access SS7/TDM Networks. This card supports simultaneous communications on up to four E1/T1 lines via front access.

The 5639L is a low profile PCIe (Peripheral Component Interconnect Express) card with 4 ports and is available with two different face plates: one for low profile PCIe slots and one for standard PCIe slots. The HP DL360 server can be configured to support the low profile and full height face plates. The HP BL460 server supports only the full height face plate.

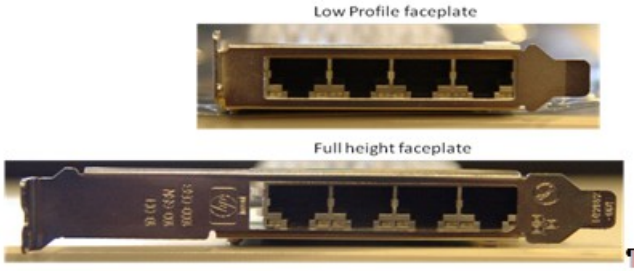


Figure 91: 5639L Interface Card face plates

Support for SS7/TDM includes

- SS7/TDM access via E1/T1
- support for up to one E1/T1 card per server, each card having 4 ports either configured as HSL or LSL
- support for configuration, maintenance, and alarms through Global Schema and WebCI
- support for SIGTRAN to be configured on the same iSPAN5639L system to provide a migration path

  Note: SIGTRAN and TDM links must be to different destinations

- integrated Interphase utilities for troubleshooting.

Cisco 3020 enclosure switch blades

Each HP c7000 enclosure can be equipped with two Cisco 3020 integrated switch blades. The Ethernet switch blades are deployed in pairs, operating in a 1+1 redundant active/active configuration.

The Cisco 3020 switch is designed with sixteen internal 1GB downlinks and eight 1GB RJ-45 copper uplinks. Up to four uplinks can be optionally configured as fiber SX links. Two uplinks can optionally be configured as internal cross-connects.

Figure 92: Cisco 3020 enclosure switch blade

Onboard administrator

The onboard administrator for the HP c7000 enclosure provides both local and remote administration of the HP c-Class system. It provides the following:

- Configuration wizard
- Access to the HP infrastructure
- Security roles for the server, network, and storage administrators
- Power and cooling of the HP infrastructure
- Agentless device health and status
- Thermal Logic power and cooling information and control

- HP Insight Display

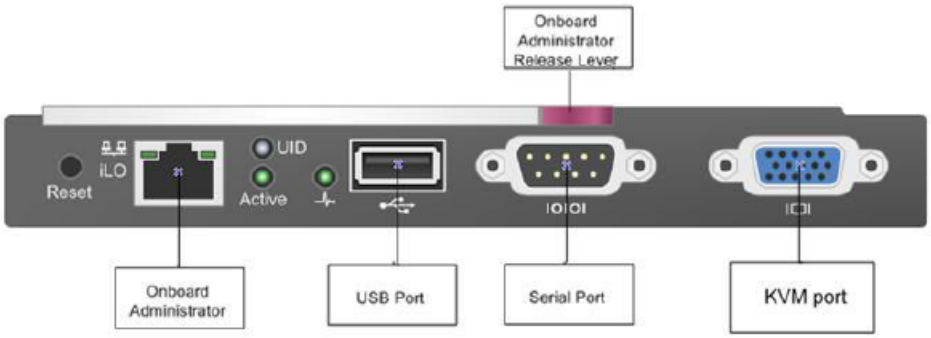


Figure 93: HP c7000 enclosure onboard administrator

Figure 94: HP Insight display

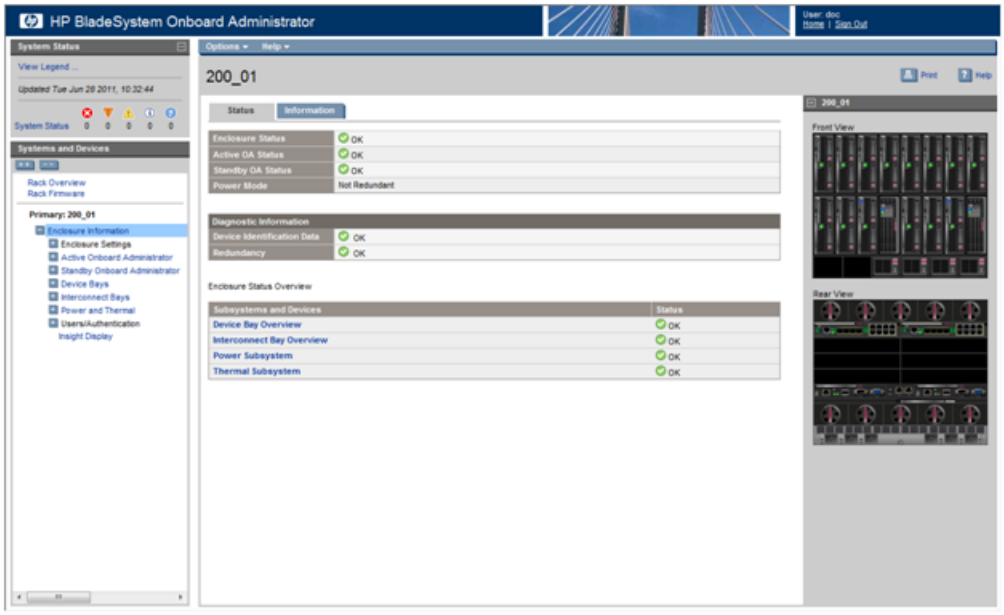


Figure 95: HP onboard administrator screen

Field replaceable unit (FRU) replacements

The HP c-Class platform supports FRU replacements for the following hardware components:

- Blade server
- Enclosure switch blade
- Hard Drives
- Power supplies
- c7000 Enclosure Fans

FRU replacements under warranty will be provided by Tekelec.

To maintain a high availability system, spare parts for key components are required.

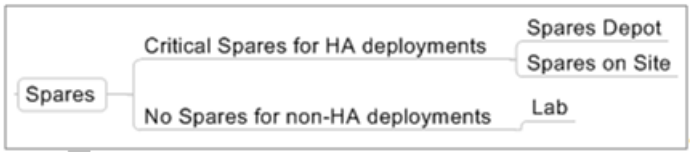


Figure 96: FRU sparing

For a cost efficient sparing strategy, a superset blade can spare for a blade of lesser capability. When spares are used, only the highest superset blade will be spared.

½ height blades shall only spare other ½ height blades and full height blades will only spare other full height blades.

For information on Field Replaceable Units (FRUs) and equipment that can be ordered for sparing, contact the *Customer Care Center*.

Chapter 11

Technical specifications

Topics:

This chapter provides technical specifications for the Subscriber Data Management system.

EAGLE XG environmental specifications

Cisco 4948E-F specifications

Table 40: Cisco 4948E-F specifications

Item	Specification
Environmental	
Operating temperature	32° to 104°F (0° to 40°C)
Storage temperature	-40° to 167°F (-40° to 75°C)
Relative humidity	10 to 90 percent, noncondensing
Operating altitude	-196 to 6561 ft (-60 to 2000m)
Air flow	28 cubic feet per minute (CFM) at low speed 44 CFM at full speed
Physical	
Dimensions	1.75 x 17.5 x 19.4 in (4.45 x 44.45 x 49.28cm)
Weight	19 lbs (8.62kg) (fully loaded with 2 PS and fan tray) 14 lbs (6.35kg)(base system only; no power supply and fan tray)
Power	
AC input voltage range	90 to 264 VAC
DC input voltage range	-40.5 to -72 VDC
Maximum Current	AC: 4 amperes (A) at 120 VAC ; 2A at 240 VAC input DC: 8 Amps @ -48 VDC input
Typical operating power	230W at 77°F (25°C)
Maximum power	275W at 131°F (55°C)
RoHS compliant	RoHS-6 compliance
Heat dissipation (Max)	AC Input: 1173 BTU/hr DC Input: 1251 BTU/hr

HP BL460 G6 specifications

Table 41: HP BL460 G6 specifications

Item	Specifications
Dimensions (H x W x D) (with bezel)	7.154 x 2.19 x 20.058 in (18.17 x 5.56 x 50.95 cm)
Weight	Maximum (all hard drives and processors installed)14.20 lb (6.44 kg) Minimum (one hard drive and processor installed)10.75 lb (4.87 kg)
Power Specifications	For power specifications including Input Requirements, BTU Rating, and Power Supply Output, refer to HP BladeSystem located at: *http://h18000.www1.hp.com/products/quickspecs/12810_na/12810_na.html* To review the typical system power ratings, use the HP BladeSystem Power Sizer tool located at *http://www.hp.com/go/bladesystem/powercalculator* Click on the system of interest and follow instructions on the screen.
System Inlet Temperature	Operating: 10° to 35°C (50° to 95°F) at sea level with an altitude derating of 1.0°C per every 305 m (1.8°F per every 1000 ft) above sea level to a maximum of 3050 m (10,000 ft), no direct sustained sunlight. Maximum rate of change is 10°C/hr (18°F/hr). The upper limit may be limited by the type and number of options installed. System performance may be reduced if operating with a fan fault or above 30°C (86°F). Non-operating: -30° to 60°C (-22° to 140°F). Maximum rate of change is 20°C/hr (36°F/hr).
Relative Humidity	Operating: 10 to 90% relative humidity (Rh), 28°C (82.4°F) maximum wet bulb temperature. Non-operating: 5 to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature.
Altitude	Operating: 3050 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1500 ft/min). Non-operating: 9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1500 ft/min).

HP BL460 Gen8 specifications

Table 42: HP BL460 Gen8 specifications

Item	Specification
Dimensions (H x W x D) (with bezel)	7.11 x 2.18 x 20.37 in (18.07 x 5.54 x 51.76 cm)
Weight	Maximum (all processors,16 DIMMs, hard drives, mezzanine cards, and two flash cache batteries installed)14.00 lb (6.33 kg) Minimum (one processor and 2 DIMMs installed)10.50 lb (4.75 kg)
Power Specifications	For power specifications including Input Requirements, BTU Rating, and Power Supply Output, refer to the HP BladeSystem located at: *http://h18000.www1.hp.com/products/quickspecs/12810_na/12810_na.html* To review the typical system power ratings, use the HP BladeSystem Power Sizer tool located at *http://www.hp.com/go/bladesystem/powercalculator* Click on the system of interest and follow the instructions of the screens.
System Inlet Temperature	Operating: 10° to 35°C (50° to 95°F) at sea level with an altitude derating of 1.0°C per every 305 m (1.8°F per every 1,000 ft) above sea level to a maximum of 3,050 m (10,000 ft), no direct sustained sunlight. Maximum rate of change is 10°C/hr (18°F/hr). The upper limit may be limited by the type and number of options installed. System performance may be reduced if operating with a fan fault or above 30°C (86°F). Non-operating: -30° to 60°C (-22° to 140°F). Maximum rate of change is 20°C/hr (36°F/hr).
Relative Humidity	Operating: 10 to 90% relative humidity (Rh), 28°C (82.4°F) maximum wet bulb temperature. Non-operating: 5 to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature.
Altitude	Operating: 3050 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1,500 ft/min). Non-operating: 9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1,500 ft/min).

HP c7000 enclosure specifications

Table 43: HP c7000 enclosure specifications

Dimensions	Height 17.4 in (442 mm) Width 17.6 in (447.04 mm) Depth 32 in (813 mm)
Shipping Dimensions	Height 29.88 in (759 mm) Width 23.88 in (607 mm) Depth 39.88 in (1013 mm)
Max Enclosure Weight (approximate)	Unboxed 450 lb (204 kg) Shipping 493 lb (223.6 kg)
Enclosure Weight (without blades)	Unboxed 151 lb (68..5 kg) Shipping 194 lb (88 kg)
Temperature Range	Operating: 50° to 95° F (10° to 35° C) Non-Operating: -22° to 140° F (-30° to 60° C)
Relative Humidity	Operating: 10 to 90% relative humidity (Rh), 28°C (82.4°F) maximum wet bulb temperature, noncondensing Non-Operating: 5 to 95% relative humidity (Rh), 38.7°C (101.7°F)maximum wet bulb temperature, noncondensing. Operating temperature has an altitude derating of 1.8° F (1° C) per 1,000 ft (304.8 m). No direct sunlight. Upper operating limit is 10,000 ft (3,048 m) or 70Kpa/10.1 psia. Upper non-operating limit is 30,000 ft (9,144 m) or 30.3 KPa/4.4 psia. Storage maximum humidity of 95% is based on a maximum temperature of 113° F (45° C). Altitude maximum for storage is 70 KPa.

HP D2200sb storage blade specifications

The HP D2200sb is a half-height storage blade with up to 12 SFF hard drives and installs in the HP c7000 enclosure.

Table 44: HP D2200sb base specifications

Feature	Description
Capacity	Up to 12 SFF Hard Disk Drives
Performance	Up to 7.2 TB Raw internal SAS
Connectivity	High-speed PCIe connection to adjacent c-Class server blade

Feature	Description
Serviceability	Hot-plug capability individual hard drives
Form Factor	Half-height single width c7000 blade

HP DL360 G6 specifications

Table 45: HP DL360 G6 specifications

Item	Specifications
Dimensions (H x W x D) (with bezel)	1.70 x 16.78 x 27.25 in (4.32 x 42.62 x 69.22 cm)
Weight	Maximum (all hard drives, power supplies, and processors installed)39.5 lb (17.92 kg) Minimum (one hard drive, power supply, and processor installed)32 lb (14.51 kg)
Power Specifications	For power specifications including Input Requirements, BTU Rating, and Power Supply Output, refer to the HP BladeSystem located at: *http://h18000.www1.hp.com/products/quickspecs/12810_na/12810_na.html* To review the typical system power ratings, use the HP BladeSystem Power Sizer tool located at *http://www.hp.com/go/bladesystem/powercalculator* Click on the system of interest and follow the instructions of the screens.
System Inlet Temperature	Operating: 10° to 35°C (50° to 95°F) at sea level with an altitude derating of 1.0°C per every 305 m (1.8°F per every 1000 ft) above sea level to a maximum of 3050 m (10,000 ft), no direct sustained sunlight. Maximum rate of change is 10°C/hr (18°F/hr). The upper limit may be limited by the type and number of options installed. System performance may be reduced if operating with a fan fault or above 30°C (86°F). NEBS short term operating temperature, 55°C Non-operating: -40° to 70° C (-40° to 158° F). Maximum rate of change is 20° C/hr (36° F/hr).
Relative Humidity	Operating: 10 to 90% relative humidity (Rh), 28°C (82.4°F) maximum wet bulb temperature, non-condensing. Non-operating: 5 to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature, non-condensing.

Item	Specifications
Altitude	Operating: 3050 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1500 ft/min). Non-operating: 9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1500 ft/min).

HP DL380 G6 specifications

Table 46: HP DL380 G6 specifications

Item	Specification
Dimensions (H x W x D) (with bezel)	3.38 x 17.54 x 27.25 in (8.59 x 44.55 x 69.22 cm)
Weight	Maximum (all hard drive, power supplies, and processors installed) 60.00 lb (27.27kg) Minimum (one hard drive, power supply, and processor installed) 47.18 lb (21.45)
Power Specifications	For power specifications including Input Requirements, BTU Rating, and Power Supply Output, refer to the HP BladeSystem located at: *http://h18000.www1.hp.com/products/quickspecs/12810_na/12810_na.html* To review the typical system power ratings, use the HP BladeSystem Power Sizer tool located at *http://www.hp.com/go/bladesystem/powercalculator* Click on the system of interest and follow the instructions of the screens.
System Inlet Temperature	Operating: 10° to 40°C (50° to 95°F) at sea level with an altitude derating of 1.0°C per every 305 m (1.8°F per every 1000 ft) above sea level to a maximum of 3050 m (10,000 ft), no direct sustained sunlight. Maximum rate of change is 10°C/hr (18°F/hr). The upper limit may be limited by the type and number of options installed. System performance may be reduced if operating with a fan fault or above 30°C (86°F). Non-operating: -30° to 60°C (-22° to 140°F). Maximum rate of change is 20°C/hr (36°F/hr).
Relative Humidity	Operating: 10 to 90% relative humidity (Rh), 28°C (82.4°F) maximum wet bulb temperature, non-condensing. Non-operating: 5 to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature, non-condensing.

Item	Specification
Altitude	Operating: 3050 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1500 ft/min). Non-operating: 9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1500 ft/min).

HP DL380 Gen8 specifications

Table 47: HP DL380 Gen8 specifications

Item	Specifications
Dimensions (H x W x D) (with bezel)	SFF Drives: 3.44 x 17.54 x 27.50 in (8.73 x 44.55 x 69.85 cm) LFF Drives: 3.44 x 17.54 x 29.50 in (8.73 x 44.55 x 74.93 cm)
Weight	Maximum (all LFF hard drives, power supply, and processors installed) 61.00 lb (27.66kg) Minimum (one SFF hard drive, power supply, and processor installed, ODD not installed) 41.0 lb (18.59 kg)
Power Specifications	For power specifications including Input Requirements, BTU Rating, and Power Supply Output, refer to the HP BladeSystem located at: *http://h18000.www1.hp.com/products/quickspecs/12810_na/12810_na.html* To review the typical system power ratings, use the HP BladeSystem Power Sizer tool located at *http://www.hp.com/go/bladesystem/powercalculator* Click on the system of interest and follow the instructions of the screens.
System Inlet Temperature	Operating: 10° to 35°C (50° to 95°F) at sea level with an altitude derating of 1.0°C per every 304.8 m (1.8°F per every 1000 ft) above sea level to a maximum of 3048 m (10,000 ft), no direct sustained sunlight. Maximum rate of change is 10°C/hr (18°F/hr). The upper limit may be limited by the type and number of options installed. System performance may be reduced if operating with a fan fault or above 30°C (86°F). Non-operating: -30° to 60°C (-22° to 140°F). Maximum rate of change is 20°C/hr (36°F/hr).
Relative Humidity	Operating: 10% to 90% relative humidity (Rh), 28°C (82.4°F) maximum wet bulb temperature, non-condensing. Non-operating: 5% to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature, non-condensing.

Item	Specifications
Altitude	Operating: 3048 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1500 ft/min). Non-operating: 9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1500 ft/min).

HP Enterprise cabinet specifications (42U)

Table 48: HP Enterprise cabinet specifications (42U)

Item	Specification
Model	HP 10642 G2
U Height	42U
Cabinet height	78.7 in. (1999 mm)
Width	23.94 in. (608 mm)
Depth	39.93 in. (999 mm)
Weight	253 lbs. (115 kg)
Max load	2000 lbs. (907 kg)
Shipping dimensions	86.22x48x36 in. (2190x1219.2x812.8 mm)
Shipping weight	307 lbs. (170 kg)

Telect seismic cabinet specifications (44U)

Table 49: Telect seismic cabinet specifications (44U)

Item	Specification
U Height	44U
Cabinet height	84 in. (2133.6 mm)
Width with side panels	24 in. (612.6 mm)
Depth	42 in. (1066.8 mm)
Max floor load	2000 lbs. (909 kg)
Seismic rating	Earthquake zone 4

Reliability

Software applications can be deployed within a site as 1+1+n, which means one master active instance for read and write with one hot standby, which can take over the active role in case of failure and n replicas for read access. Specific configurations vary depending on the product being deployed.

Operating system

Tekelec Platform Distribution (TPD) is a standard Linux-based OS built and distributed by Tekelec. TPD provides value-added features for managing installations and upgrades, diagnostics, integration of 3rd party software (open and closed source), build tools, and server management tools.

Web browser

The Web Craft Interface (WebCI) supports the following versions of web browsers:

- Internet Explorer version 8 on Windows.
- Mozilla Firefox version 12.0.

Glossary

#

3GPP	3rd Generation Partnership Project

A

AAA	Authentication, Authorization, and Accounting
AC	Alternating Current
APN	Access Point Name The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.
AS	Application Server A logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination. The AS contains a set of one or more unique Application Server Processes, of which one or more normally is actively processing traffic.
ASE	Application Service Element
ATI	Any Time Interrogation An ATI message allows an external server to interrogate an HLR and

A

obtain information about the location and/or state of a GSM subscriber.

AuC — Authentication Center

AVP — Attribute-Value Pair

The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.

C

CdPA — Called Party Address

The field in the SCCP portion of the MSU that contains the additional addressing information of the destination of the MSU. Gateway screening uses this additional information to determine if MSUs that contain the DPC in the routing label and the subsystem number in the called party address portion of the MSU are allowed in the network where the EAGLE 5 ISS is located.

CEA — Capability-Exchange-Answer

The Diameter response that the prepaid rating engine sends to the Mobile Originated application during capability exchanges.

CER — Capabilities-Exchange-Request

A Diameter message that the Mobile Originated application sends to a prepaid rating engine to

C

	perform a capability exchange. The CER (indicated by the Command-Code set to 257 and the Command Flags' 'R' bit set) is sent to exchange local capabilities.The prepaid rating engine responds with a Capability-Exchange-Answer (CEA) message.
CLI	Command-line interface
CSCF	Call Session Control Function
CSV	Comma-separated values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).
CUG	Closed User Group

D

DHCP	Dynamic Host Configuration Protocol
Diameter	Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless

D

	type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.
DNS	Domain Name System A system for converting Internet host and domain names into IP addresses.
DRA	Destination Routing Address
DSF	Domain Selection Function
DSR	Diameter Signaling Router A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

E

EA	Expedited Data Acknowledgment
EIR	Equipment Identity Register A network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). Use of the EIR can prevent the use of stolen handsets because the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being

E

	registered on the network, thus making them useless.
ENUM	T**E**lephone **NU**mber **M**apping
EPC	Emulated Point Code

F

FMC	Fixed-Mobile Convergence
FQDN	Fully qualified domain name The complete domain name for a specific computer on the Internet (for example, www.tekelec.com).

G

Gateway GPRS Support Node	See GGSN.
GGSN	Gateway GPRS Support Node An edge router that acts as a gateway between a GPRS wireless data network and other networks. The MPE supports GGSN nodes as network elements. See also GPRS, PGW, and SGW.
GPRS	General Packet Radio Service A mobile data service for users of GSM mobile phones.
GSM	Global System for Mobile Communications
GTT	Global Title Translation A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE 5 ISS uses to determine which service database

G

	to send the query message when an MSU enters the EAGLE 5 ISS and more information is needed to route the MSU. These service databases also verify calling card numbers and credit card numbers. The service databases are identified in the SS7 network by a point code and a subsystem number.

H

HLR	Home Location Register
HSL	High-Speed Link
HSS	Home Subscriber Server A central database for subscriber information.

I

IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identifier
IMS	IP Multimedia Subsystem These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication.
IMSI	International Mobile Subscriber Identity

I

IPSP	IP Server Process A process instance of an IP-based application. An IPSP is essentially the same as an ASP, except that it uses MU3A in a peer-to-peer fashion. Conceptually, an IPSP does not use the services of a signaling gateway.
IPv4	Internet Protocol version 4
ISO	International Standards Organization
ITU	International Telecommunications Union

L

LOC	The primary function of the LOC server is to locate subscribers on GSM and IS-41 networks.
LSL	Low-speed Link
LTE	Long Term Evolution The next-generation network beyond 3G. In addition to enabling fixed to mobile migrations of Internet applications such as Voice over IP (VoIP), video streaming, music downloading, mobile TV, and many others, LTE networks will also provide the capacity to support an explosion in demand for connectivity from a new generation of consumer devices tailored to those new mobile applications.

M

M3UA	SS7 MTP3-User Adaptation Layer

M

	M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MAP	Mobile Application Part
MNP	Mobile Number Portability
MS	Mobile Station The equipment required for communication with a wireless telephone network.
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.
MSRN	Mobile Station Roaming Number
MTP	Message Transfer Part The levels 1, 2, and 3 of the SS7 protocol that control all the functions necessary to route an SS7 MSU through the network

N

NAI	Network Access Identifier The user identity submitted by the client during network authentication.
NAS	Network Access Server

N

	A single point of access or gateway to a remote resource. NAS systems are usually associated with AAA servers.
NDC	Network destination code
NE	Network Element An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location. Network Entity
Network Element	See NE
NPDB	Number Portability Database
NSP	Network Services Part The lower layers of the SS7 protocol, comprised of the three levels of the Message Transfer Part (MTP) plus the signaling Connection Control Part (SCCP), are known collectively as the Network Services Part (NSP).

O

OAM	Operations, Administration, and Maintenance The application that operates the Maintenance and Administration Subsystem which controls the operation of many Tekelec products.
OAM&P	Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.

O

	Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability. Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics). Provisioning – Setting up user accounts, devices, and services.
OP	Operation
opaque data	A data type whose specific schema is not defined as a part of the interface, but rather is handled as a unit and not interpreted or parsed. The values within opaque data can only be manipulated by calling subroutines that have specific knowledge of the structure/schema of the data.
OSI	Open System Interconnection The International Standards Organization (ISO) seven layer model showing how data communications systems can be interconnected. The seven layers, from lowest to highest are: **1.** Physical layer **2.** Datalink layer **3.** Network layer **4.** Transport layer **5.** Session layer **6.** Presentation layer **7.** Application layer

O

OSS	Operator Specific Services

P

PDN	Packet Data Network A digital network technology that divides a message into packets for transmission.
PDP	Power Distribution Panel Monitors primary and secondary power sources on a continuous basis.
PLMN	Public Land Mobile Network
PUR	Profile Update Request on Sh Interface Command sent by a Diameter client to a Diameter server in order to update user data in the server.

Q

quota	Specifies restrictions on the amount of data volume, active session time, or service-specific events that a subscriber can consume.

R

RADIUS	Remote Authentication Dial-In User Service A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

R

realm	A fundamental element in Diameter is the realm, which is loosely referred to as domain. Realm IDs are owned by service providers and are used by Diameter nodes for message routing.
RFC	Request for Comment RFCs are standards-track documents, which are official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group the IESG.
RN	Routing Number

S

SAAL	Signaling ATM Adaptation Layer
SAE	Service Action Execution
SAP	Service Access Point Shelf Alarm Panel
SBC	Session Border Controller Device used in some VoIP networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down calls.
SCCP	Signaling Connection Control Part
S-CSCF	Serving - Call Session Control Function

S

	Provides user and service authentication and authorization, client registration, SIP-routing capabilities, service integration, data management, FW/NAT traversal, multi-network integration and an interface to third-party applications.
SCTP	Stream Control Transmission Protocol An IETF transport layer protocol, similar to TCP that sends a message in one operation. The transport layer for all standard IETF-SIGTRAN protocols. SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SDM	Subscriber Data Management
SDS	Subscriber Data Server Provides new ways of accessing, extracting, and finding value from subscriber data, and thus enables operators to leverage the wealth of subscriber information previously fragmented all over their network. By simplifying the management of subscriber data and profiling customer behavior, the Subscriber Data Server allows carriers to exploit real-time data, deliver monetized personalized services, and even bind to third part services easily.

S

SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SM	Short Message
SMS	Short Message Service
SNR	Subscriber Notification Request on Sh Interface
SOAP	Simple Object Access Protocol
SPR	Subscriber Profile Repository A logical entity that may be a standalone database or integrated into an existing subscriber database such as a Home Subscriber Server (HSS). It includes information such as entitlements, rate plans, etc. The PCRF and SPR functionality is provided through an ecosystem of partnerships.
SS	Supplementary Services
SS7	Signaling System #7
SSH	Secure Shell A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to

S

	effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.
SSR	SIP Signaling Router Function responsible for querying a redirection server and proxying requests to other SSR servers, redirect servers, SSR Service Points, and Gateways. It helps in evolving a Flat NGN network into a hierarchical network.
Subscriber Data Management	See SDM.
System Manager	Server with hardware management software that manages the remaining servers (System OAMs and MPs) in a network element. The terms PM&C and system manager are used synonymously in the online help documentation.

T

TCAP	Transaction Capabilities Application Part
TCP	Transfer Control Protocol
TDP	Trigger Detection Point
Tekelec Platform Distribution	See TPD.
TPD	Tekelec Platform Distribution TPD is a standard Linux-based operating system packaged and distributed by Tekelec. TPD provides value-added features for managing installations and

T

	upgrades, diagnostics, integration of 3rd party software (open and closed source), build tools, and server management tools.
TPS	Transactions Per Second

U

UDP	User Datagram Protocol
UE	User Equipment
UL	Underwriters Laboratories
UMTS	Universal Mobile Telecommunications System The standard for 3G used by GSM service providers. UMTS includes voice and audio services, for fast data, graphic and text transmissions, along with transmission of moving images and video.
URI	Uniform Resource Identifier An internet protocol element consisting of a short string of characters that conform to a certain syntax. The string comprises a name or address that can be used to refer to a resource.
URL	Uniform Resource Locator
USM	User Security Management

U

USSD	Unstructured Supplementary Service Data

V

VCC	Voice Call Continuity The 3GPP has defined the Voice Call Continuity (VCC) specifications in order to describe how a voice call can be persisted, as a mobile phone moves between circuit switched and packet switched radio domains.
VLR	Visitor Location Register A component of the switching subsystem, within a GSM network. The switching subsystem includes various databases which store individual subscriber data. One of these databases is the HLR database or Home Location Register; and the VLR is another.
VMSC	Visited MSC Voice Mail Service Center
VoIP	Voice Over Internet Protocol Voice communication based on the IP protocol competes with legacy voice networks, but also with Voice over Frame Relay and Voice and Telephony over ATM. Realtime response, which is characterized by minimizing frame loss and latency, is vital to voice communication. Users are only prepared to accept minimal delays in voice transmissions.

W

WebCI	Web Craft Interface

X

XML	eXtensible Markup Language A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.