Oracle® Communications Convergent Charging Controller

SIP Compliance for Session Control Agent

Release 6.0

May 2016

ORACLE®

Copyright

Contents

Introduction

This document details the IETF Request for Comment (RFC) against which the Session Control Agent (SCA) is compliant with. The compliance to the RFCs relates to the SCA Session Initiation Protocol (SIP) interface and message exchange.

These RFCs are listed below:

- **RFC 1123** – Requirements for Internet hosts – application and support
- **RFC 2327** – SDP: Session Description Protocol
- **RFC 2782** – A DNS RR for specifying the location of services
- **RFC 2806** – URLs for Telephone Calls
- **RFC 2916** – E.164 numbers and DNS
- **RFC 3261** – SIP: Session Initiation Protocol
- **RFC 3262** – PRACK : Reliability of provisional responses in SIP
- **RFC 3265** – Session Initiation Protocol (SIP)-Specific Event Notification
- **RFC 3264** – An Offer/Answer Model with the Session Description Protocol (SDP)
- **RFC 3311** – The Session Initiation Protocol (SIP) UPDATE Method
- **RFC 3325** – Private Extensions to SIP for Asserted Identity within Trusted Networks
- **RFC 3326** – The Reason Header Field for the Session Initiation Protocol (SIP)
- **RFC 3398** – ISDN ISUP to SIP mapping
- **RFC 3455** – Private Header (P-Header) Extension to the SIP for 3GPP
- **RFC 3725** – Third-party call control in SIP

In addition, this document details the compliance of the SCA INAP interface against the ETS 300 374 INAP standard.

The following are popular SIP RFCs typically supported by MGW and reasons for SCA not claiming compliance to them:

- **RFC 2833** – RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
  - The SLC SCA does not terminate or generate RTP streams since it is an AS.
- **RFC 2976** – The SIP INFO Method
  - The SCA does not intelligently process INFO messages but transparently passes these messages between. The support of this feature will be considered for a future release to trigger service events.
- **RFC 3323** – A Privacy Mechanism for the Session Initiation Protocol (SIP)
  - SLC SCA is typically deployed within a trusted network environment within a telecommunications operator network domain. Where the telecommunications network interfaces to a public network (e.g. internet), it is the responsibility of the operator to ensure that information entering its network is from trusted sources. Therefore, there are no special privacy mechanisms implemented by the SLC. However, privacy information contained within SIP messages exchanged through SLC are respected.
- **RFC 3515** – The Session Initiation Protocol (SIP) Refer Method

- REFER messages transparently passed by SCA. REFER is typically exchanged between endpoints to perform operations such as call transfer. There is no need for the SLC to process these, so these messages are transparently passed.

- **RFC 3891** – The Session Initiation Protocol (SIP) "Replaces" Header
  - Transparently passed by SLC. Typically used by end points or switches to modify dialogue information e.g. name/number of terminal that is currently dealing with the call/session if the user has transferred the call. Not supported by SLC, because SLC platform relies on core network to perform supplementary services such as transfer so there is no need for it to inject this header into messages.

1. RFC 1123 – Requirements for Internet hosts – application and support

The SCA is fully compliant with the RFC 1123. This is applicable to allow telnet sessions to enable remote tracing of ongoing dialogues.

2. RFC 2327 – SDP – Session Description Protocol

The SCA supports processing of SDP information into an appropriate bearer value that can be used to influence charging.

3. RFC 2782 – A DNS RR for specifying the location of services

The SCA is fully compliant with the RFC 2782. The SCA uses DNS to resolve URL domain names.

4. RFC 2806 – URLs for Telephone Calls

The SCA is fully compliant with the RFC 2806. Support for non-hexadecimal URLs must be agreed with the customer.

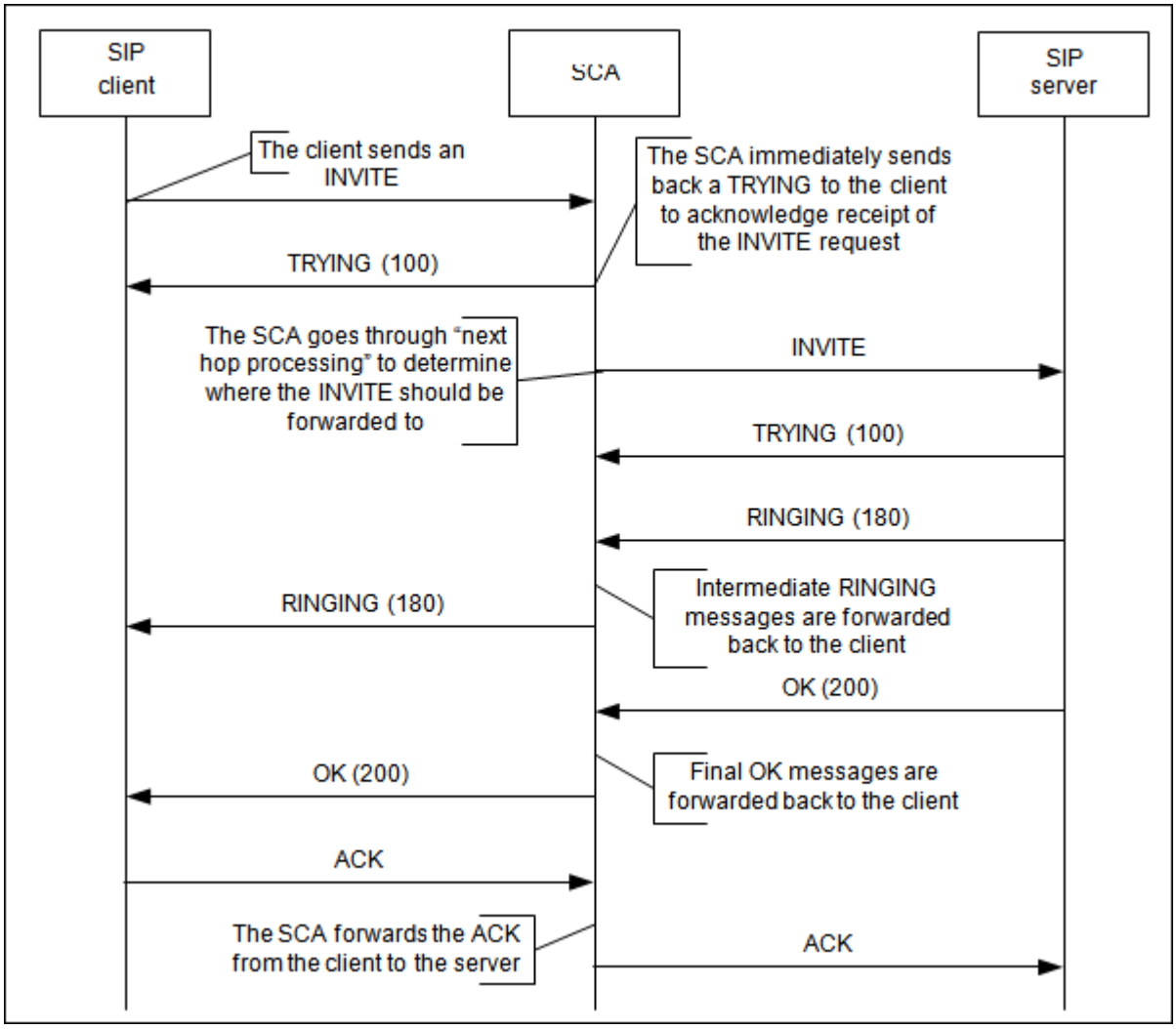
5. RFC 2916 – E.164 numbers and DNS

The SLC offers the ENUM product that provides full compliance of RFC 2916. The SCA can use the SLC ENUM DB to map tel URLs into general URLs.

6. RFC 3261 – SIP: Session Initiation Protocol

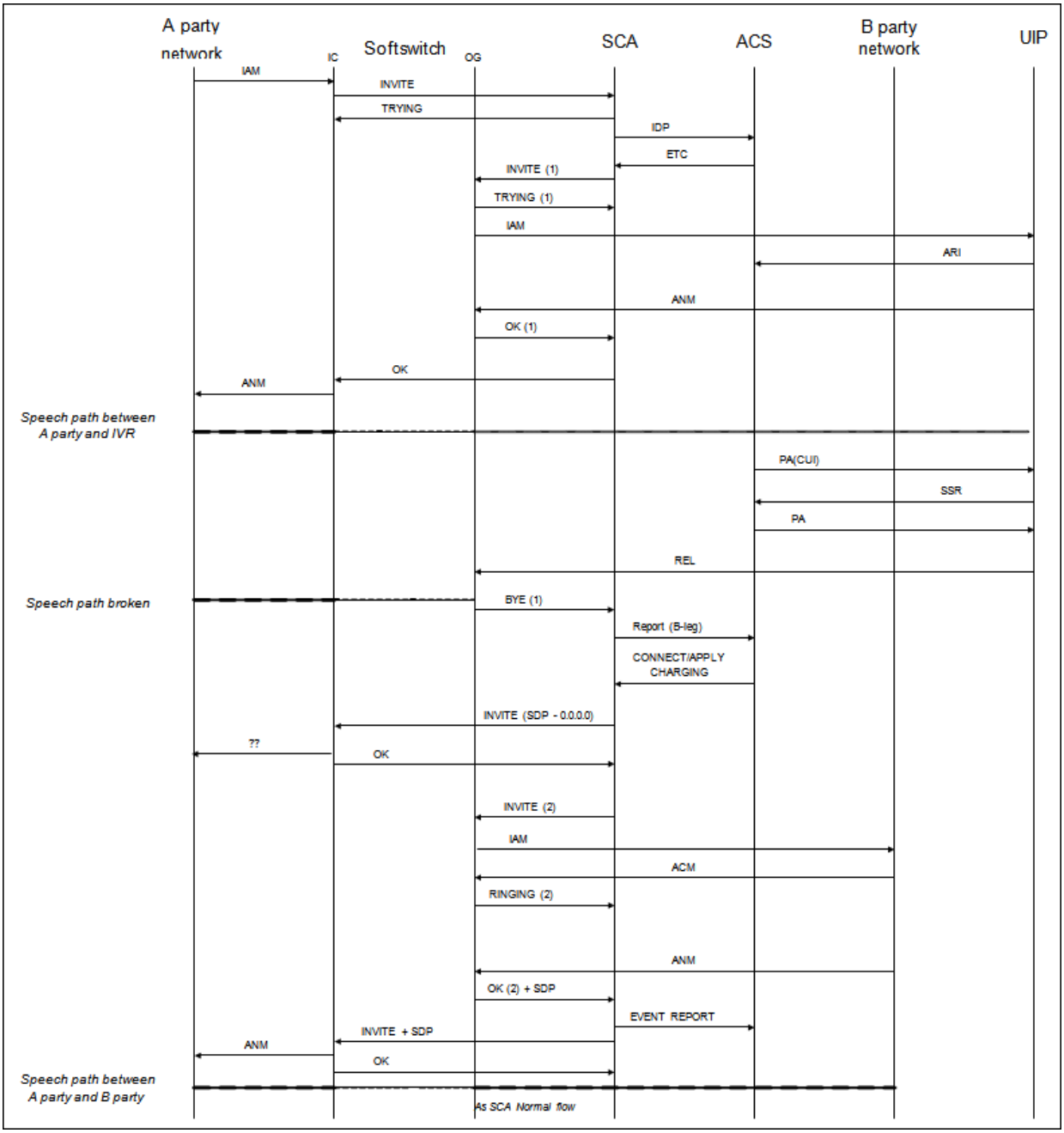
The SCA is partially compliant with the RFC 3261. Basic call/session flow supported by SCA and based upon RFC 3261 recommendations are shown below:

Figure 1. Basic call/session setup flow



The following diagram shows a more advanced control flow still using principles in 3261:

Figure 2. Advanced call flow, IVR session with UIP then connect to destination



The following SIP messages are required for SCA operation.

Table 1. SCA RFC 3261 SIP message support

SIP MESSAGE	SoftSwitch -> SCA	SCA -> SoftSwitch
ACK	R	R
BYE	R	R
CANCEL	R	R
INVITE	R	R
OPTION	R	R
REGISTER	R	R

The SCA is not compliant with the following sections of RFC 3261:

Table 2. SCA RFC 3261 non-supported areas

Section	Description
19.1	SIP and SIPS Uniform Resource Indicators
19.1.1	SIP and SIPS URI Components
19.1.3	Example SIP and SIPS URIs
20.44	WWW-Authenticate
22	Usage of HTTP Authentication
22.1	Framework
22.2	User-to-User Authentication
22.3	Proxy-to-User Authentication
22.4	The Digest Authentication Scheme
23	S/MIME
23.1	S/MIME Certificates
23.2	S/MIME Key Exchange
23.3	Securing MIME bodies
23.4	SIP Header Privacy and Integrity using S/MIME: Tunnelling SIP
23.4.1.2	Confidentiality
23.4.2	Tunnelling Integrity and Authentication
23.4.3	Tunnelling Encryption
26	Security Considerations: Threat Model and Security Usage Recommendations
26.1	Attacks and Threat Models
26.1.1	Registration Hijacking
26.1.2	Impersonating a Server
26.1.3	Tampering with Message Bodies
26.1.5	Denial of Service and Amplification
26.2	Security Mechanisms
26.2.1	Transport and Network Layer Security
26.2.2	SIPS URI Scheme
26.2.3	HTTP Authentication
26.2.4	S/MIME
26.3	Implementing Security Mechanisms

Section	Description
26.3.1	Requirements for Implementers of SIP
26.3.2	Security Solutions
26.4	Limitations
26.4.1	HTTP Digest
26.4.2	S/MIME
26.4.3	TLS
26.4.4	SIPS URIs
26.5	Privacy
27	IANA Considerations
27.5	The "message/sip" MIME type

The exclusions are related to security. It is presumed that the SCA will operate in a trusted network, and that there will be elements such as firewalls and session border controllers between the trusted network and potentially hostile networks and devices.

7. RFC 3262 – Reliability of provisional responses in SIP

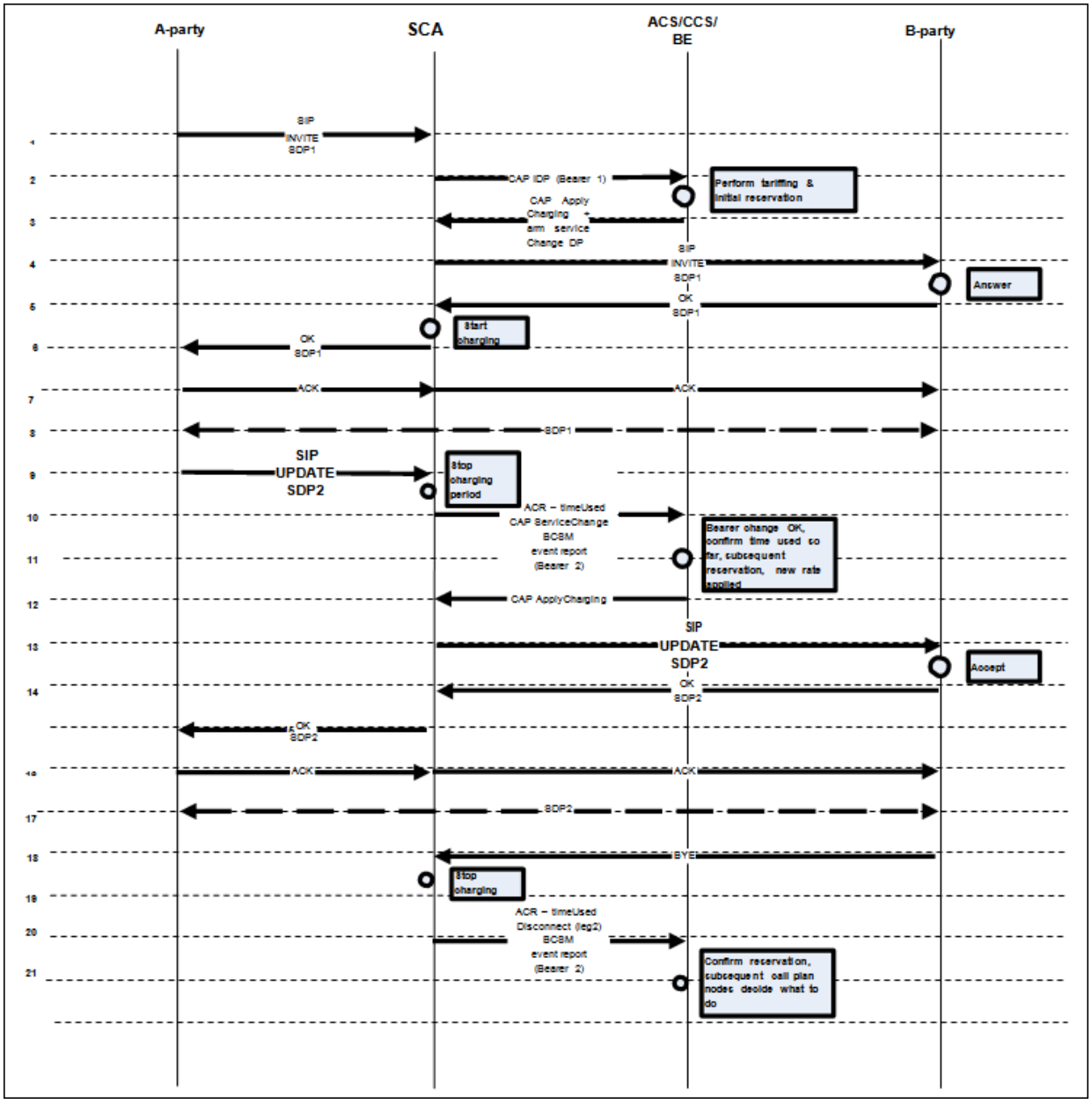
The SCA supports 3262 as follows:

- Support for PRACK in the SCA shall be optional and is turned off by default
- With PRACK support disabled, the SCA shall accept incoming PRACKs and will return 200 OK responses to the PRACKs received
- With PRACK support enabled, the SCA returns a PRACK when it receives a non-100 provisional response

8. RFC 3264 – An Offer/Answer Model with the Session Description Protocol (SDP)

The SCA supports the offer/answer model for bearer negotiation during session establishment. The SCA supports bearer session re-negotiation during session initiation and modifies charging rate appropriately as shown in the following diagram:

Figure 3. SCA support of session renegotiation and tariff change



9. RFC 3265 – Session Initiation Protocol (SIP)-Specific Event Notification

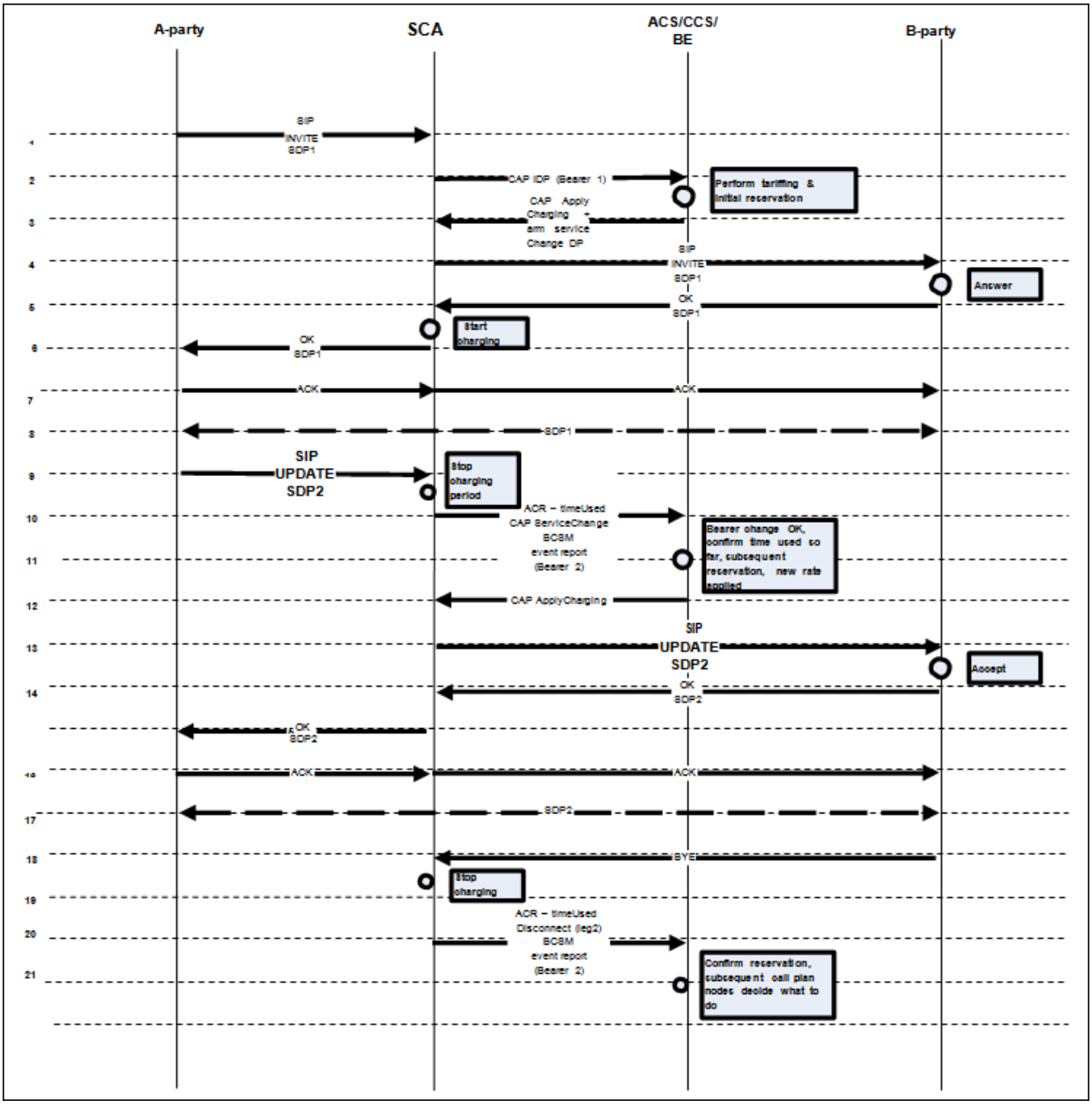
SIP Event notification, SCA in conjunction with ACS presence functionality (presence pack) supports.

The SUBSCRIBE/NOTIFY message exchange will work in a synchronous fashion with currently no support for asynchronous NOTIFY. This service relies on an external presence server.

10. RFC 3311 – The Session Initiation Protocol (SIP) UPDATE Method

The SCA supports the UPDATE method for changing media details during a session and modifying charging rate appropriately as shown in the following diagram:

Figure 4. SCA Support of RFC 3311 using UPDATE and tariff change



11. RFC 3325 – Private Extensions to SIP for Asserted Identity within Trusted Networks

The SCA is compliant with RFC 3325 for P-Asserted-Identity field.

12. RFC 3326 – The Reason Header Field for the Session Initiation Protocol (SIP)

The SCA supports the REASON header field in the SIP BYE message.

13. RFC 3372 and RFC 3398 – Session Initiation Protocol for Telephones (SIP-T)

The SCA can decode the ISUP messages in the SIP MIME parts. Current support is for:

- **ISUP IAM:** Nature Of Address and Relocation numbers for mapping into the service
- **ISUP REL:** Can obtain release cause and send to service

All other values will be obtained from the SIP headers, i.e. Calling and Called party numbers.

14. RFC 3455 – Private Header (P-Header) Extension to the SIP for 3GPP

The SCA is fully compliant with the RFC 3455.

The SCA supports P-Asserted Identity as a means of identifying the calling party, but is not compliant to the Private ID aspects of the RCF.

15. RFC 3725 – Third-party call control in SIP

The SCA is fully compliant with the RFC 3725. ACS can be used to initiate a session.

16. INAP compliance – ETS 300 374

The SCA is compliant with the ETS 300 374 for the INAP interface.

17. Error Codes and Release Causes

The following Error codes and Release causes are supported:

If a CS1 InitialDP sent to an external IN application results in a CS1 ReleaseCall being received back, an error is returned to the SIP client. The SIP response code depends on the INAP release cause (see table below for a mapping). The Reason-Phrase will end with the string "(INAP *xx*)", where *xx* is the decimal release cause extracted from the CS1 ReleaseCall component.

Table 3. SIP error message to ISUP release cause mapping

INAP release cause	SIP response code
1 unallocated number	404 Not Found
2 no route to network	404 Not found
3 no route to destination	404 Not found
17 User busy	486 Busy here

INAP release cause	SIP response code
18 no user responding	408 Request Timeout
19 no answer from the user	480 Temporarily unavailable
20 subscriber absent	480 Temporarily unavailable
21 Call rejected	603 Decline
22 number changed (w/o diagnostic)	410 Gone
22 number changed (with diagnostic)	301 Moved Permanently
23 redirection to new destination	410 Gone
26 non-selected user clearing	404 Not Found
27 destination out of order	502 Bad Gateway
28 address incomplete	484 Address incomplete
29 facility rejected	501 Not implemented
31 Normal	404 Not found
34 no circuit available	503 Service unavailable
38 network out of order	503 Service unavailable
41 Temporary failure	503 Service unavailable
42 switching equipment congestion	503 Service unavailable
47 resource unavailable	503 Service unavailable
55 incoming calls barred within CUG	403 Forbidden
57 bearer capability not authorized	403 Forbidden
58 bearer capability not presently available	503 Service unavailable
65 bearer capability not implemented	488 Not Acceptable Here
70 only restricted digital available	488 Not Acceptable Here
79 service/option not implemented	501 Not implemented
87 user not member of CUG	403 Forbidden
88 incompatible destination	503 Service unavailable
102 recovery on timer expiry	504 Gateway timeout
111 protocol error	500 Server internal error
127 interworking unspecified	500 Server internal error

In addition, the Reason header field of the SIP response will be populated as follows:

`Reason: Q.850; cause=<xx>`

where <*xx*> is the INAP release cause found in the ReleaseCall component.

Glossary of Terms

ACS

Advanced Control Services

ASP

Application Services Provider

PAM

Presence and Availability Manager

SCA

Session Control Agent

SIP

Session Initiation Protocol