Oracle® Communications Service Broker

Security Guide

Release 6.0

E26766-01

March 2012

Oracle Communications Service Broker Security Guide, Release 6.0

E26766-01

Contents

Preface v

Audience v
Documentation Accessibility v
Related Documents v
Downloading Oracle Communications Documentation v

1 Service Broker Security Overview

Basic Security Considerations 1-1
Overview of Service Broker Security 1-1
Oracle Security Documentation 1-2
Understanding the Service Broker Environment 1-2

2 Implementing Service Broker Security

About the Service Broker Security Model 2-1
Implementing Service Broker Securely 2-1
Changing Default Ports 2-2
Securing Passwords 2-3
Securing Clusters 2-4
Configuring Domain Security in the Service Broker Property Files 2-4
Securing Managed Servers 2-5
Set Up the Public Key Infrastructure 2-5
Set Up a Credential Store 2-5
Set Up Network Communication End Points 2-5
Securing Service Broker with Firewalls 2-5
Securing Network Traffic with Protocol-Specific Security 2-6
HTTPS Protocol Required for Production 2-6
Securing the SVC and VPN Features 2-7
Securing the SVC Feature 2-8
Securing the VPN Feature 2-8
Securing the Online Mediation Controller Feature 2-8
Securing Network Communication 2-8
SS7 SIGTRAN 2-9
SS7 TDM 2-9
SIP 2-9
Diameter 2-9

Radius 2-10
SMPP 2-10
PCP (Oracle BRM) 2-10
Web Services (SOAP or REST over HTTP) 2-10
Monitoring Service Broker Events 2-11

3 Security Considerations for Service Broker Developers

Securing Your Applications 3-1

Preface

This document describes the Oracle Communications Service Broker security features and procedures.

Audience

This document is intended for system administrators and system integrators who install and configure Service Broker, and integrate it with existing telecom networks, and developers who will add features and capabilities to Service Broker.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Communications Release 6.0 documentation set:

- *Oracle Communications Service Broker System Administrator's Guide*
- *Oracle Communications Service Broker Installation Guide*

Oracle documentation is available from Oracle Technology Network:

`http://docs.oracle.com`

Downloading Oracle Communications Documentation

Oracle Communications Service Broker documentation is available from the Oracle software delivery Web site:

`http://edelivery.oracle.com/`

Additional Oracle Communications documentation is available from Oracle Technology Network:

http://www.oracle.com/technetwork/index.html

1

Service Broker Security Overview

This chapter provides an overview of how to configure and manage security for the Oracle Communications Service Broker (Service Broker) product.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date**. This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible**. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity**. Establish who should access which system components, and how often, and monitor those components.
- **Install software securely**. For example, use firewalls, secure protocols such as SSL and secure passwords.
- **Learn about and use the Service Broker security features**. See these sections for details:
    - Configuring Security between Service Broker Components in *Oracle Communications Service Broker System Administrator's Guide*.
    - Securing Credentials with Credential Store in *Oracle Communications Service Broker System Administrator's Guide*.
- **Use secure development practices**. For example, take advantage of existing database security functionality instead of creating your own application security. See "Security Considerations for Service Broker Developers" for more information.
- **Keep up to date on security information**. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Overview of Service Broker Security

Service Broker relies on these lines of defense against malicious attacks:

- High-level protection from the individual protocols that it supports. The "Implementing Service Broker Security" chapter goes into details on how to set up protocol-specific security features.

- Low-level (packet-based) protection using firewalls that you select, obtain, and configure to use with Service Broker. Every Service Broker implementation is different and you need to assess and obtain firewalls that meet you implementation's needs.
- Service Broker's built-in security features, such as configurable password strength, and native keystores and truststores for storing credentials. See "Implementing Service Broker Security" for details on how to implement these features.
- The policies and procedures that you put in place for configurable software security. This chapter provides some guidance in for these policies and procedures, but every Service Broker implementation is different and you need to consult your security expert for the best way to completely secure yours.

Oracle Security Documentation

To implement security, Service Broker uses other Oracle products, such as an Oracle Database. See the following documents for more information:

- *Oracle Database Security Guide*.
- *Oracle Database Advanced Security Administrator's Guide*.
- *Billing and Revenue Management System Administrator's Guide*.
- *Oracle Coherence Release 3.7 Developer's Guide*, section *Operational Configuration Elements*.
- *Oracle Coherence Security Guide.*

Understanding the Service Broker Environment

When planning your Service Broker implementation, consider the following:

- Which resources need to be protected?
  - You need to protect customer data, such as credit-card numbers.
  - You need to protect internal data and traffic, such as billing event traffic.
  - You need to protect system components from being disabled by external attacks or intentional system overloads
- Who are you protecting data from?

  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might needs to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage you system components without needing to access the system data
- What will happen if protections on a strategic resources fail?

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

2 Implementing Service Broker Security

This chapter describes the security model for Oracle Communications Service Broker and explains how to configure it.

About the Service Broker Security Model

Service Broker is a flexible product designed to community with a wide variety of other network nodes and applications. Consequently the there are also a wide variety of security concerns when dealing with Service broker security that explained in "Implementing Service Broker Securely".

This chapter assumes that you have already installed the operating system required by Service Broker, and then installed Service Broker itself. For details see *Oracle Communications Service Broker Installation Guide*.

By default Service Broker is configured to be as secure as possible. If you disabled any of these security settings to create a test and evaluation system, be sure enable them before starting a productions implementation

Implementing Service Broker Securely

This section describes recommended deployment configurations for a secure Service Broker implementation. Configure Service Broker security with these steps:

1. Install the operating system that Service Broker runs on.

   The first step in creating a Service Broker implementation is to install the operation system it runs on. See your operating system documentation for instructions on how to install it securely. Also see "Basic Security Considerations"

2. Install Service Broker.

   See *Oracle Communications Service Broker Installation Guide* for details on installation. By default Service Broker is configured to be as secure as possible. You may have disabled these security settings when you created a test and evaluation system. Be sure enable the security settings before starting a productions implementation.

3. Change the default ports. See "Changing Default Ports" for details.
4. Maintain a high level of password security. See "Securing Passwords" for details.
5. (As needed) Secure clusters. See "Securing Clusters" for details.
6. Configure domain security settings with the Service Broker properties files. See "Configuring Domain Security in the Service Broker Property Files" for information.

7. Secure the Service Broker Managed Servers. See "Securing Managed Servers" for details.
8. Set up a Public Key Infrastructure to store SSL/TLS credentials. See "Set Up the Public Key Infrastructure" for information.
9. (As needed) Set up Credential Store for storing non-keystore credentials. See "Set Up a Credential Store" for information.
10. Set up telecom protocol traffic security. See "Set Up Network Communication End Points" for details.
11. Configure your server firewalls. See "Securing Service Broker with Firewalls" for details.
12. Configure your Service Broker network entry points, routing, and aliases (IMs, OE, and SSUs). See "Set Up Network Communication End Points" for details.
13. (As needed) Configure protocol security support. See "Securing Network Traffic with Protocol-Specific Security" for details.
14. Configure security for other Oracle products. See "Related Documents" for details.

These steps are explained in the sections that follow.

Changing Default Ports

After installing Service Broker be sure to change all the default ports, and continue doing so as you complete the post installation steps listed in *Oracle Communications Service Broker Installation Guide*.

Table 2–1 lists the default server port numbers that Service Broker uses by default and where to change them.

Table 2–1 Service Broker Default Server Ports

Component/Protocol	Port Number	Description
Administration Console (Web)	9001 for HTTPS 9000 for HTTP	Set in the **hosting.properties** and **web.properties** property files. See the system administrator's reference in *Oracle Communications Service Broker System Administrator's Guide* for details.
Policy Designer Interface	8091 for HTTPS 8090 for HTTP	Set in the **oracle.ocsb.app.rcc.pcrf.gui.port** or **pcrf.gui.http.port.secure** system properties. For details see the discussion on configuring Service Broker for Policy Controller in *Oracle Communications Service Broker Policy Controller Implementation Guide*.
Admin Port (for Administrator Console to Managed Server communication)	8901 for HTTPS 8900 for HTTP	Set in the **Admin Port** entry when creating a Managed Server. For details see the discussion on post installation tasks in *Oracle Communications Service Broker Installation Guide*.
Managed Server JMX JRMP port	10003	Set in the **JMX JRMP port** entry when creating a Managed Server. For details see the discussion on post installation tasks in *Oracle Communications Service Broker Installation Guide*
JMX Registry port	10103	Set in the **JMX Registry port** entry when creating the Managed Server. For details see the discussion on post installation tasks in *Oracle Communications Service Broker Installation Guide*

Table 2–1 (Cont.) Service Broker Default Server Ports

Component/Protocol	Port Number	Description
Log4J socket server port	4096	The **common.properties** property file. See the system administrator's reference in *Oracle Communications Service Broker System Administrator's Guide* for details.
IP Multicast port	1024	Set in the **common.properties** property file. See the system administrator's reference in *Oracle Communications Service Broker System Administrator's Guide* for details.
Multicast Port	1025	The **common.properties** property file. See the system administrator's reference in *Oracle Communications Service Broker System Administrator's Guide* for details.
Profile Database Server IP	1521	Set in SSU WEB SERVICES. For details see the discussion on enabling subscriber profile service connectivity in *Oracle Communications Service Broker Subscriber Store User's Guide*.
Diameter	3588	Set in the SSU DIAMETER. For details see the discussion on configuring Diameter signaling server units in *Oracle Communications Service Broker Signaling Domain Configuration Guide*.
Radius	1812-Authentication 1813-Accounting	You set a range of NAS ports to use in the Radius SSU. For details see the discussion on configuring RADIUS signaling server units in *Oracle Communications Service Broker Signaling Domain Configuration Guide*.
HTTP	None	Set in SSU WEB SERVICES. For details see the discussion on configuring the web services signaling server units in *Oracle Communications Service Broker Signaling Domain Configuration Guide*.
SMPP	None	Set in the SSU SMPP. For details see the discussion on configuring SMPP signaling server units in *Oracle Communications Service Broker Signaling Domain Configuration Guide*.
SS7	None	Set in one of the SS7 SSU, depending on the SS7 protocol used. For details see the discussion on configuring the SS7 Signaling Server Unit for your protocol in *Oracle Communications Service Broker Signaling Domain Configuration Guide*.
SIP	5060	Set in the SIP SSU. For details see the discussion on configuring SIP signaling server units in *Oracle Communications Service Broker Signaling Domain Configuration Guide*

Securing Passwords

There are no default password that you need to change. Passwords are all created by you during installation.

Service Broker provides a high level of flexibility in securing the Web Administration Console password by using the **common.properties** file settings. For example, you can change required password length, or its requirement to include an integer. See the system administrator's reference in *Oracle Communications Service Broker System Administrator's Guide* for details on the settings.

Securing Clusters

You secure the Coherence cluster using the standard Coherence configuration settings.

Oracle recommends that you secure the cluster by creating a Coherence configuration override file, packaging it as an OSGI bundle fragment and deploying it.

For more information on concepts of the Coherence security, refer to *Oracle Coherence 3.7 Security Guide.*

For information on how to create a Coherence configuration override file and details on the available security options, see *Oracle Coherence Release 3.7 Developer's Guide*, section *Operational Configuration Elements*, and *Oracle Coherence Security Guide*.

Both documents are available from *Oracle Coherence Knowledge Base*:

http://coherence.oracle.com/display/COH/Oracle+Coherence+Knowledge+Base+Home

The Coherence operational override configuration file must be named **tangosol-coherence-override-axia.xml** in order to complement, rather than replace, the override settings already defined by Service Broker.

For information on how to create an OSGi bundle fragment, refer to *OSGi Service Platform Release 4 Core specification*, section *3.14 Fragment Bundles*. The specification can be downloaded from:

http://www.osgi.org/Release4/Download

The fragment host for the OSGi fragment bundle must be **oracle.axia.storage.provider.coherence**.

Configuring Domain Security in the Service Broker Property Files

Service Broker collects it's processing and signalling servers into *domains* the are protected first by the firewalls that secure your physical server, second by HTTPS security, and finally using file system-level security within the server.

In *Oracle Communications Service Broker System Administrator's Guide*, see the discussion about domains for general information about domains, and the discussions on domain configuration security and hosted domain security for specifics on protecting Service Broker domains.

Most of Service Broker's application-facing security settings are contained in these property files:

- *Oracle_home*/**ocsb60/admin_console/properties**
  - **common.properties** - Contains property settings that control all actions associated with the Administration Console, which means this is where most of Service Broker's security settings are.
  - **hosting.properties** - Contains properties settings that control hosted domains. See the discussion on security for the domain configuration in *Oracle Communications Service Broker System Administrator's Guide* for details.
  - **script.properties** - Contains properties settings for the scripting engine
  - **standalone.properties** - Contains property settings for a standalone Web Administration Console.

  - **web.properties** - Contains property settings for the web Administration Console server.

- *Domain_home*/*Domain_name*/**domain.properties** - contains domain-specific properties settings. Do not change any of these settings, they are not configurable.
- *Oracle_home*/**ocsb60/managed_server/server.properties** - Contains properties settings for the Managed Server.

For a listing and descriptions of the security settings in these files, see:

- The system administrators reference appendix in *Oracle Communications Service Broker System Administrator's Guide*.
- The properties files themselves.

Securing Managed Servers

Each Managed Server contains a **server.properties** file in *Oracle_home*/**managed_server** that contains security settings such as a truststore name to use hostname verification. Make changes to these settings before starting and running a production Service Broker implementation. For details see the system administrator's reference in *Oracle Communications Service Broker System Administrator's Guide*.

Set Up the Public Key Infrastructure

You use the **keytool** program to create the public key infrastructure (PKI) keystores and truststores required for Service Broker to communicate with applications and web entities that support SSL. For details on setting up the PKI see these discussions on configuring security between Service Broker components in *Oracle Communications Service Broker System Administrator's Guide*.

Set Up a Credential Store

Service Broker provides a Credential Store feature to store credentials for applications and protocols that use username/password credentials or keystores for access. For details on setting up the Credential Store, see securing credentials with Credential Store for in *Oracle Communications Service Broker System Administrator's Guide*.

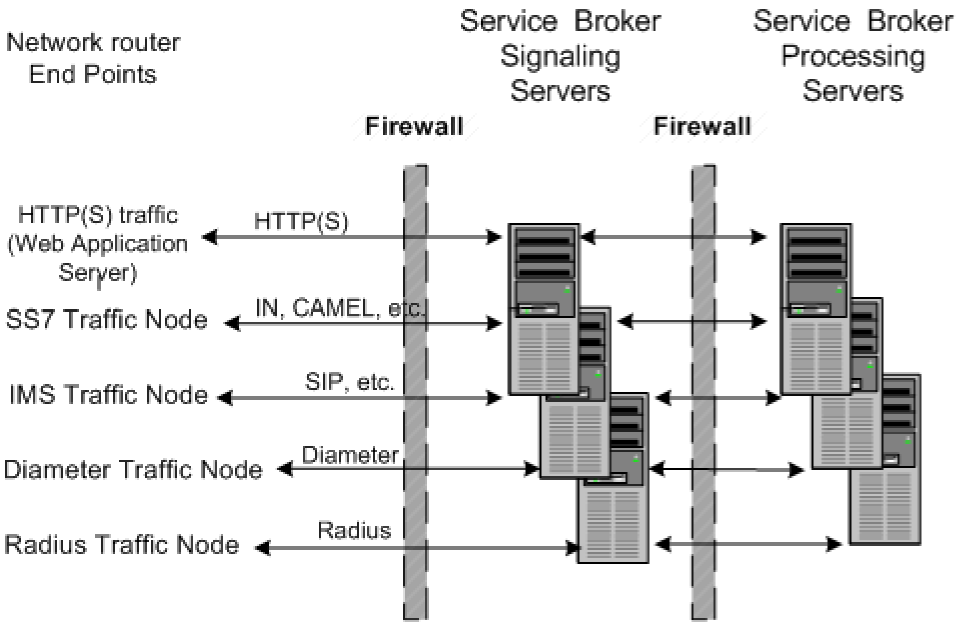
Set Up Network Communication End Points

Service Broker communicates with Telecom networks using a variety of supported IMS and SS7-based protocols. You secure communication with network elements by creating Signaling Server Units (SSUs) that are network communication end points for the network traffic. Each protocol SSU has its own security features based on the individual precool. See "Securing Network Communication" for details on securing traffic for individual protocols.

Securing Service Broker with Firewalls

Figure 2–1 shows a typical Service Broker production deployment. Oracle recommends that you protect Service Broker from security risks by configuring firewalls between each the Service Broker processing layers, and between Service Broker and any network traffic. See your firewall product documentation for information on how to set them up with Service Broker.

Figure 2–1 Service Broker Security Architecture Overview



Securing Network Traffic with Protocol-Specific Security

Because Service Broker supports a variety of Protocols, it relies on the security features of those individual protocols for higher-level security support. The combination of firewall protection and protocol-level security support protect Service Broker from network security risks.

The Service Broker Service controller features mediate between various telecom network protocols. Securing communication protocols mainly involves creating virtual "white lists" of trusted systems to communicate with.

HTTPS Protocol Required for Production

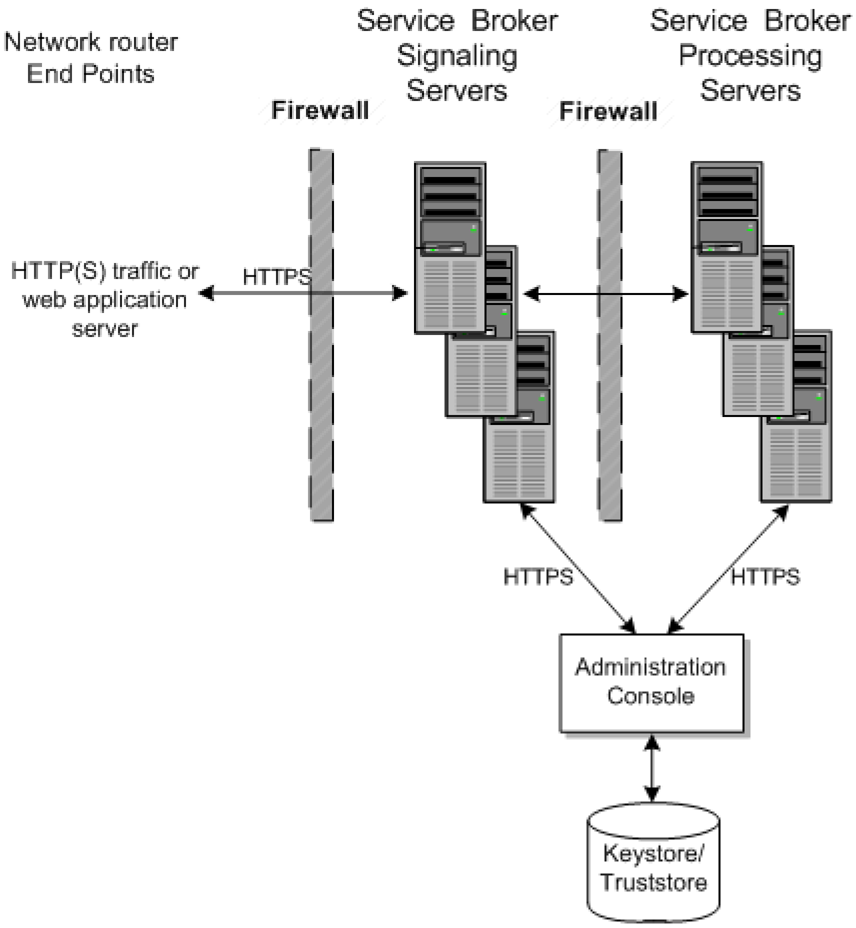
You have the option of using either HTTP or HTTPS for test and evaluation Service Broker implementations, but production implementations must use the security provided by HTTPS/SSL/TLS. All web applications that you use with Service Broker must support HTTPS/SSL/TLS features.

The HTTPS/SSL/TLS network traffic that passes to Service Broker is protected by HTTPS/SSL/TLS security, and all applications and internet entities must support HTTPS to work with Service Broker.

During installation, you configure the keystores and truststores that Service Broker uses to authenticate HTTPS traffic. Figure 2–2 shows how the Service Broker SSU and PN servers share the stores. See *Oracle Communications Service Broker System Administrator's Guide* for details on setting the keystores and truststores up.

Service Broker also includes a Credential Store feature for programs that use username/password credentials instead of HTTPS-style certificates (for example, LDAP servers). See *Oracle Communications Service Broker System Administrator's Guide* for details on setting up Credential Stores.

Figure 2–2 Service Broker HTTPS Keystores and Truststores

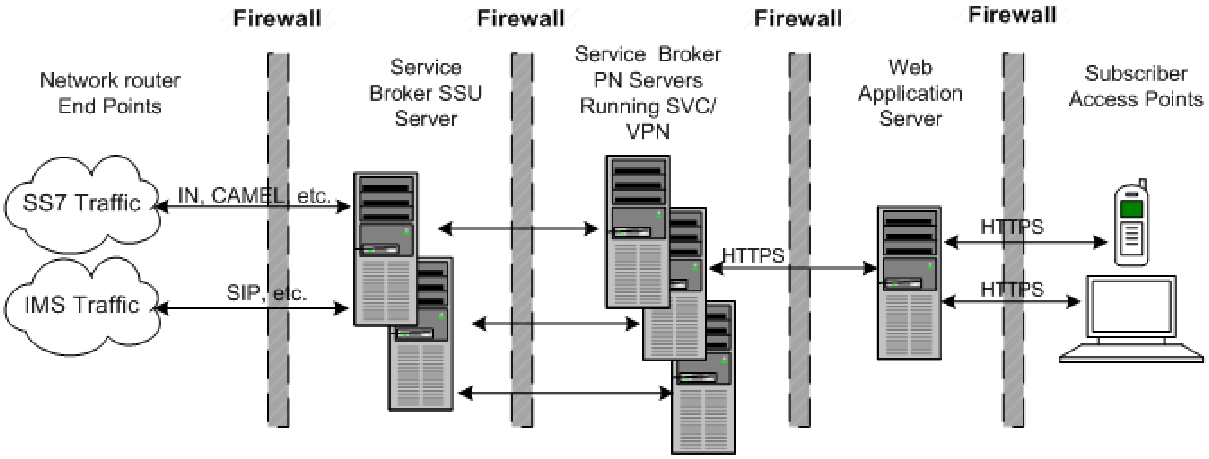


Securing the SVC and VPN Features

The Service Broker SVC feature application runs inside of Service Broker so it is protected from your web application server and Internet nodes by two layers of firewall and HTTPS support.

Figure 2–3 shows a Service Broker implementation with the SVC and VPN features configured. Both of these features run inside Service Broker in a Processing Server. The Processing Server executes the RESTful interface that these features are base on. Once set up, your subscribers access the SVC/VPN features through a web interface that you create and run on a web application server. This diagram illustrates the firewalls required to secure them. Your subscribers access the web interface using the HTTPS protocols. See "Set Up the Public Key Infrastructure" for details on setting up the PKI required to use HTTPS.

Figure 2–3 Service Broker SVC/VPN Security Overview



Securing the SVC Feature

Other than requiring HTTPS and an additional firewall to protect the web application server, there are no special security considerations for using this feature. See *Oracle Communications Service Broker SVC Implementation Guide* for details on how to set up and use this feature, and the remainder of this chapter for instructions on how to implement a secure Service Broker.

Securing the VPN Feature

The Service Broker VPN feature requires HTTPS and an additional firewalls to protect the web application server that your subscribers use to access this feature. Also see *Oracle Communications Service Broker VPN Implementation Guide* for other security considerations.

Securing the Online Mediation Controller Feature

If you use the Online Mediation Controller to mediate between Service Broker and your online charging application, see these documents for instructions on how to set it up securely:

- Your online charging application's documentation.
- The "Securing Network Communication" section.
- The discussion on setting up RADIUS Mediation for Authentication and Authorization in the Radius in *Oracle Communications Service Broker Online Mediation Controller Implementation Guide*.

Securing Network Communication

This section explains the protocol-specific security features that Service Broker uses to communicate securely over networks using supported protocols. Service Broker implements protocol security features in the signaling domain. Service Broker provides a Signaling Server Unit (SSU) for each supported protocol that you use to configure the protocol, including security. An SSU might contain session timers, encryption choices, client port number or other protocol-specific security parameters. parameters. The SSUs include:

- SS7 - SIGTRAN M3UA
- SS7 - TDM
- SIP
- Diameter
- Radius
- SMPP
- PCP (Oracle Communications BRM)
- Web Services (HTTP using SOAP or REST)

You configure these SSUs using either the Administration Console or the corresponding Java MBeans exposed for this purpose.

For details on these SSUs and how to configure them, see *Oracle Communications Service Broker System Administrator's Guide*.

The following sections list the security options that you configure for each protocol.

SS7 SIGTRAN

You use the SSU SS7 SIGTRANN or the Java MBeans operations and parameters to set up security by specifying M3UA layer, trusted SCCP sites, and incoming routing rules for SIGTRAN network traffic. See the discussion on configuring SIP Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details.

SS7 TDM

You use the SSU SS7 SIGTRANN or the Java MBeans to set up security by specifying MTP connectivity and mapping, SCCP addresses, and incoming routing rules for TDM network traffic. See configuring the SS7 Signaling Server Units for TDM in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details.

SIP

You use the SSU SS7 SIGTRAN or the corresponding Java MBeans to set up security by specifying trusted SIP network entities that use SIP network channels you specify. See configuring SIP Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details.

In addition, Oracle recommends that you implement security measures appropriate to your implementation, such as:

- Implement the IPsec protocol between the system running Service Broker and the network nodes.
- Use TLS tunneling between the network node and Service Broker by implementing a load balancer/firewall (such as an F5 load balancer) at the DMZ that performs hardware acceleration/offloading on the secured connection from the firewall to the external network element.

Diameter

You use the SSU Diameter or the corresponding Java MBeans to set up security by specifying trusted nodes and peers, and creating routing rules for their network traffic.

See configuring Diameter Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details.

In addition, Oracle recommends that you implement security measures appropriate to your implementation, such as:

- Implement the IPsec protocol between the system running Service Broker and the network nodes.
- Use TLS tunneling between the network node and Service Broker by implementing a load balancer/firewall (such as an F5 load balancer) at the DMZ that performs hardware acceleration/offloading on the secured connection from the firewall to the external network element.

Radius

You use the Service Broker SSU Radius or the corresponding Java MBeans to set up security by specifying trusted clients to accept accounting and authentication requests from. The SSU Radius also supports the Service Broker Credential Store feature for storing username/password credentials for Radius users.

See configuring Diameter Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details on configuring the SSU Radius. See securing credentials with Credential Store in *Oracle Communications Service Broker System Administrator's Guide* for details on using the Credential Store.

SMPP

You use the Service Broker SMPP SSU or the corresponding MBeans to set up security by specifying trusted Short Message Service Centers (SMSCs) and the Extended Short Message Entities (ESMEs) they connect to.

See configuring SMPP Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details. See securing credentials with Credential Store in *Oracle Communications Service Broker System Administrator's Guide* for details on using the Credential Store.

PCP (Oracle BRM)

You use the Service Broker SSU PCP or the corresponding MBeans to set up security by specifying a trusted Oracle BRM connection manager (CM) to connect Service Broker to. You specify the specific CM pool ID, host, port, etc., that identifies the CM. The SSU PCP also support the Service Broker Credential Store feature for storing username/password credentials the BRM requires.

See configuring PCP Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details. See securing credentials with Credential Store in *Oracle Communications Service Broker System Administrator's Guide* for details on using the Credential Store

Web Services (SOAP or REST over HTTP)

You use the Service Broker SSU Web Services to specify trusted web entities that Service Broker communicates with by specifying incoming and outgoing routing rules. You also set up HTTP network access points (addresses and ports) for your trusted nodes to use, and SSL security (keystore and truststores to use for authenticating connections). The SOAP and HTTP protocols support the Service Broker Credential Store feature for storing username/password credentials to authenticate traffic.

See configuring Web Services Signaling Server Units in *Oracle Communications Service Broker Signaling Domain Configuration Guide* for details. See securing credentials with Credential Store in *Oracle Communications Service Broker System Administrator's Guide* for details on using the Credential Store

Monitoring Service Broker Events

You may choose to monitor Service Broker events, such as creating a VPN administrative user, or changing user permissions, using its runtime MBeans. For details on setting up monitoring, see the monitoring Service Broker discussion in *Oracle Communications Service Broker System Administrator's Guide*.

3

Security Considerations for Service Broker Developers

This chapter provides information for developers about how to create secure applications for Service Broker and how to extend Service Broker without compromising security

Securing Your Applications

The Service Broker Service Controller features allow you to serve applications to telecom networks supporting a variety of protocols. The most secure applications support SSL/TLS *and* use certificates to authenticating network traffic. Oracle recommends that you also always implement credential security even when the traffic is protected by SSL/TLS. Oracle recommends that you not serve applications on Service Broker unless they use at least one of these two security strategies.

See your application's documentation for information on how to set it up to use the Service Broker security features listed in "Implementing Service Broker Security".