Oracle® Communications Services Gatekeeper

SDK User Guide

Release 4.1

January 2009

ORACLE

Oracle Communication Services Gatekeeper SDK User Guide, Release 4.1

Contents

Installing and Configuring the SDK

Workshop Controls with Oracle Communications Services Gatekeeper

CHAPTER 1

Document Roadmap

The following sections describe the audience for, and organization of, this document:

Document Scope and Audience

This guide describes the operation of the Oracle Communications Services Gatekeeper SDK, including:

- Supported functionality
- Installation, start up and configuration
- General operation

The intended audience consists of developers and test engineers developing applications that will interact with Oracle Communications Services Gatekeeper.

Guide to This Document

This document contains the following chapters:

- Chapter 1, “Document Roadmap”: This chapter
- Chapter 2, “Oracle Communications Services Gatekeeper SDK”: Introduction to the Oracle Communications Services Gatekeeper Simulator
- Chapter 3, “Using the Oracle Communications Services Gatekeeper SDK”: How to use the Oracle Communications Services Gatekeeper Simulator
- Chapter 4, “Installing and Configuring the SDK”: Installing the Oracle Communications Services Gatekeeper Simulator
- Chapter 5, “Workshop Controls with Oracle Communications Services Gatekeeper”: Using Workshop controls with Oracle Communications Services Gatekeeper

Terminology

The following terms and acronyms may be used in this document:

- 3GPP—3rd Generation Partnership Project, a collaborative group of telecom standards bodies
- Account—A registered application or service provider. An account belongs to an account group, which is tied to a common SLA.
- Account group—Multiple registered service providers or applications that share a common SLA
- Administrative user—Someone who has privileges on the Oracle Communications Services Gatekeeper management tool. This person has an administrative user name and password.
- Alarm—The result of an unexpected event in the system, often requiring corrective action.
- API—An application programming interface
- Application—A TCP/IP based, telecom-enabled program accessed from either a telephony terminal or a computer
- Application-facing interface—The interface that Application Service Providers use to interact with Oracle Communications Services Gatekeeper
- Application Service Provider—An organization offering application services to end users through a telephony network
- AS—An application server

- Application Instance—An Application Service Provider from the perspective of internal Oracle Communications Services Gatekeeper administration. An Application Instance has a user name and a password
- CBC—Charging based on the nature of the content delivered, not on time used or simple per-use cost. Content based charging.
- CDR—Charging Data Record
- Communication Service—A facade and an enabler that together form the path through which requests travel in Oracle Communications Services Gatekeeper. Each communication service corresponds to a particular service capability.
- CORBA—Common Object Request Broker Architecture
- CPU—Central Processing Unit
- CRM—Customer Relationship Management
- DMZ—Demilitarized Zone, a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network
- EAR—Enterprise Archive file
- EJB—Enterprise Java Bean
- Enabler—The Oracle Communications Services Gatekeeper layer that performs policy evaluation, routing, and protocol translation. It provides network-facing interfaces.
- End user—The ultimate consumer of the services that an application provides. An end user can be the same as the network subscriber, as in the case of a prepaid service or the end user can be a non-subscriber, as in the case of an automated mail-ordering application where the subscriber is the mail-order company and the end user is a customer to this company
- Enterprise Operator—See Application Service Provider
- Enterprise Service Bus—A middleware component that supports messaging, routing, XML data transformation, and service orchestration
- ETSI—The European Telecommications Standards Institute, a telecom standards body
- Event—A traceable, expected occurrence in the system, of interest to the operator
- EDR—Event Data Record

- EWS—Extended Web Services, a set of Web Services interfaces developed by Oracle offering access to network functionality not covered by Parlay X.
- Facade—A set of interfaces exposed to application service developers. A facade functions as a view of an enabler.
- HA—Mechanisms set up to insure high availability
- HTML—Hypertext Markup Language
- HTTP—Hypertext Transfer Protocol
- INAP—Intelligent Network Application Part, a telephony signalling protocol
- Interceptor Stack—A flexible set of chained evaluation steps used in Oracle Communications Services Gatekeeper
- IP—Internet Protocol
- JDBC—Java Database Connectivity, the Java API for database access
- JEE—Java Enterprise Edition
- JMS—Java Message Service
- JMX—Java Management Extensions
- LDAP—Lightweight Directory Access Protocol
- Location Uncertainty Shape—A geometric shape surrounding a base point specified in terms of latitude and longitude. It is used in terminal location.
- MAP—Mobile Application Part
- Marshall— Record the state and codebase(s) of an object in such a way that when the marshalled object is "unmarshalled," a copy of the original object is obtained, possibly by automatically loading the class definitions of the object.
- Mated pair—Two physically distributed installations of Oracle Communications Services Gatekeeper nodes sharing a subset of data allowing for high availability between the nodes
- MIB—Management Information Base
- MLP—Mobile Location Protocol
- MM7—A multimedia messaging protocol specified by 3GPP

- MMS—Multimedia Message Service or an instance of this service
- MMSC—Multimedia Message Service Center
- Network plug-in—The Oracle Communications Services Gatekeeper module that implements the interface to a network node or OSA/Parlay SCS through a specific protocol
- NS—Network Simulator
- OAM—Operation, Administration, and Maintenance
- OASIS—The Organization for the Advancement of Structured Information Standards, an e-business and web standards consortium
- OCSG—Oracle Communications Services Gatekeeper
- Operator—The party that manages Oracle Communications Services Gatekeeper. Usually the network operator
- On-boarding—Registering applications and service providers to enable their access to Oracle Communications Services Gatekeeper and the underlying network
- ORB—Object request broker
- OSA/Parlay—The Open Service Access interfaces used by a Parlay gateways
- OSS—Operation Support Systems
- Out of the box—The level of functionality available in the default installation of Oracle Communications Services Gatekeeper
- PAP—Push Access Protocol
- Parlay—The Parlay Group, a telecom standards body
- Parlay Gateway—A telecom gateway implementing Parlay interfaces
- Parlay X—A set of telecom Web Services interfaces specified by the Parlay Group
- Plug-in—See Network Plug-in
- Plug-in Manager—The OCSG module charged with routing an application-initiated request to the appropriate network plug-in
- POJO—Plain Old Java Object

- Presence information—A status indicator that conveys the accessibility and the willingness of a potential communication partner
- Presentity—A supplier of presence information.
- PRM—Partner Relationship Management
- Quotas—An access rule based on an aggregated number of invocations. See also Rates
- RAM—Random Access Memory
- RAID—Redundant Array of Independent Disks
- Rates—An access rule based on allowable invocations per time period. See also Quotas
- RESTful—Interfaces that follow Representation State Transfer style
- Rf—The Diameter offline charging mode
- RMI—Remote Method Invocation
- Ro—The Diameter online charging mode
- SAML—Security Assertion Markup Language
- SCF—Service Capability Function or Service Control Function, in the OSA/Parlay sense.
- SCS—Service Capability Server, in the OSA/Parlay sense. Oracle Communications Services Gatekeeper can interact with these on its network-facing side
- Service Capability—Support for a specific kind of traffic within Oracle Communications Services Gatekeeper. Defined in terms of communication services
- SIP—Session Initiation Protocol
- SLA—A service level agreement
- SMPP—Short Message Peer-to-Peer Protocol
- SMS—Short Message Service, or an instance of this service
- SMSC—Short Message Service Center
- SNMP—Simple Network Management Protocol
- SOA—Service Oriented Architecture
- SOAP—A protocol for exchanging Web Services messages

- SPI—Service Provider Interface
- SQL—Structured Query Language
- SS7—Signalling System #7, a signaling protocol used in traditional telecom networks
- Subscriber—A person or organization that signs up for access to an application. The subscriber is charged for the application service usage. See End user
- TCP—Transmission Control Protocol
- TUPS—Transaction Units Per Second
- URI—Uniform Resource Identifier
- URL—Uniform Resource Locator
- USSD—Unstructured Supplementary Service Data
- VAS—Value Added Service
- VASP—Value Added Service Provider
- VLAN—Virtual Local Area Network
- VPN—Virtual Private Network
- W3C—The World Wide Web Consortium, a web standards group
- WAP Push—A protocol for sending WAP content (an encoded message including a link to a WAP address) that is pushed to a subscriber's handset
- Watcher—A consumer of presence information
- WS-Security—An OASIS security standard for Web Services
- WSDL —Web Services Definition Language
- XML—Extensible Markup Language

Related Documentation

This SDK user guide is a part of the Oracle Communications Services Gatekeeper documentation set. The other documents include:

- *System Administrator's Guide*

- *Concepts and Architectural Overview*
- *Installation Guide*
- *Integration Guidelines for Partner Relationship Management*
- *Managing Accounts and SLAs*
- *Statement of Compliance and Protocol Mapping*
- *Application Development Guide*
- *Communications Services Reference*
- *Handling Alarms*
- *Licensing*
- *Platform Development Studio - Developer's Guide*
- *RESTful Application Development Guide*
- *Platform Test Environment*

Additionally, many documents in the Oracle WebLogic Server documentation set are of interest, including:

- *Introduction to Oracle WebLogic Server* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/intro/
- *Getting Started With WebLogic Web Services Using JAX-WS* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/webserv/index.html

CHAPTER 2

Oracle Communications Services Gatekeeper SDK

Introduction to the Oracle Communications Services Gatekeeper SDK

The Oracle Communications Services Gatekeeper SDK provides a simulator for Oracle Communications Services Gatekeeper and an interactive, graphical test environment for developers who are creating SOAP- based applications to interact with Oracle Communications Services Gatekeeper. The current version of the Oracle Communications Services Gatekeeper Simulator supports the Parlay X 2.1 Short Messaging, Multimedia Messaging, Terminal Location interfaces, and the Extended Web Services WAP Push interfaces.

The Oracle Communications Services Gatekeeper SDK is used for functional testing. Because it simulates a Oracle Communications Services Gatekeeper, it is not necessary to have an active instance of Oracle Communications Services Gatekeeper when developing and performing functional tests of applications.

The following sections provide an overview of the Oracle Communications Services Gatekeeper SDK:

What the Oracle Communications Services Gatekeeper Simulator Provides

The Oracle Communications Services Gatekeeper Simulator offers the following capabilities:

Supported interfaces

- Extended Web Services Access
- Extended Web Services Session Manager

  Note: It is also possible to use the Simulator in "sessionless" mode. See the "Interacting with Oracle Communications Services Gatekeeper" chapter in the *Application Development Guide* for more information on session and sessionless modes.
- Parlay X 2.1 Short Messaging
- Parlay X 2.1 Multimedia Messaging
- Parlay X 2.1 Terminal Location
- Extended Web Services WAP Push

Supported message types

- SMS
- MMS
  - Text: plain text, HTML, and WML text only messages.
  - Graphics: gif, wbmp, tiff, png, and jpeg graphic files.
  - Applications: multipart, multipart-mixed, and SMIL.
- WAP Push

Supported Network Simulation

Network triggered events

Network triggered events, such as messages sent from a mobile phone to an application, can be simulated, using the Oracle Communications Services Gatekeeper Simulator GUI.

The following events are supported:

- Receive SMSes
- Receive MMSes
- Periodic Terminal Location notifications

Application triggered requests

Application triggered requests, such as messages sent from the application to a mobile phone in the network, can be simulated, including:

- All request functionality from the application to Oracle Communications Services Gatekeeper.
- All call back functionality from Oracle Communications Services Gatekeeper to the application.

Other tasks

- Adding and deleting mobile phones
- Setting the geographical position of a mobile phone
- Adding application accounts for application login
- Provisioning of off-line notifications

What the Oracle Communications Services Gatekeeper SDK Comprises

The Oracle Communications Services Gatekeeper SDK is built up of these main parts:

- A simulator, including application-facing telecom interfaces
- A simulator GUI
- Workshop Controls for telecom Web Services

The Oracle Communications Services Gatekeeper Simulator

The Oracle Communications Services Gatekeeper Simulator simulates a subset of the functionality of Oracle Communications Services Gatekeeper. From an application point-of-view, the Simulator acts as a Oracle Communications Services Gatekeeper that has connectivity to the telecom network. The Simulator provides an abstracted high-level simulation of the underlying network, with mobile terminals that can send and receive messages.

The Oracle Communications Services Gatekeeper Simulator Application-Facing Interfaces

The Oracle Communications Services Gatekeeper Simulator exposes a subset of the interfaces and methods that Oracle Communications Services Gatekeeper exposes:

- Parlay X 2.1 Interface SendSms:
  - sendSms
  - sendSmsLogo (only a binary representation of the logo is sent.)
  - sendSmsRingtone (only a binary representation of the ringtone is sent.)
  - getSmsDeliveryStatus
- Parlay X 2.1 Interface SmsNotification:
  - notifySmsReception
  - notifySmsDeliveryReceipt
- Parlay X 2.1 Interface ReceiveSms:
  - getReceivedSms
- Parlay X 2.1 Interface SmsNotificationManager:
  - startSmsNotification
  - stopSmsNotification
- Parlay X 2.1 Interface SendMessage:
  - sendMessage
  - getMessageDeliveryStatus

- Parlay X 2.1 Interface ReceiveMessage:
  - getReceivedMessages
  - getMessage
- Parlay X 2.1 Interface MessageNotification:
  - notifyMessageReception
  - notifyMessageDeliveryReceipt
- Parlay X 2.1 Interface MessageNotificationManager:
  - startMessageNotification
  - stopMessageNotification
- Parlay X 2.1 Interface TerminalLocation:
  - getLocation
  - getTerminalDistance
  - getLocationForGroup
- Parlay X 2.1 Interface TerminalLocationNotificationManager:
  - startPeriodicNotification
  - endNotification
- Parlay X 2.1 Interface TerminalLocationNotification:
  - locationNotification
  - locationError
  - locationEnd
- Extended Web Services WAP Push Interface PushMessage:
  - sendPushMessage
- Extended Web Services WAP Push Interface PushMessageNotification:
  - resultNotificationMessage
- Session Manager Service, Interface Session Manager
  - getSession

  - destroySession
  - refreshSession
  - getSessionRemainingLifeTime
  - changeApplicationPassword

- Access Service, Interface Access:

  Deprecated interface. This version of Oracle Communications Services Gatekeeper Simulator is backward compatible with Network Gatekeeper 2.2 Access service for authentication and session management. New applications should use the Session Manager Service instead.

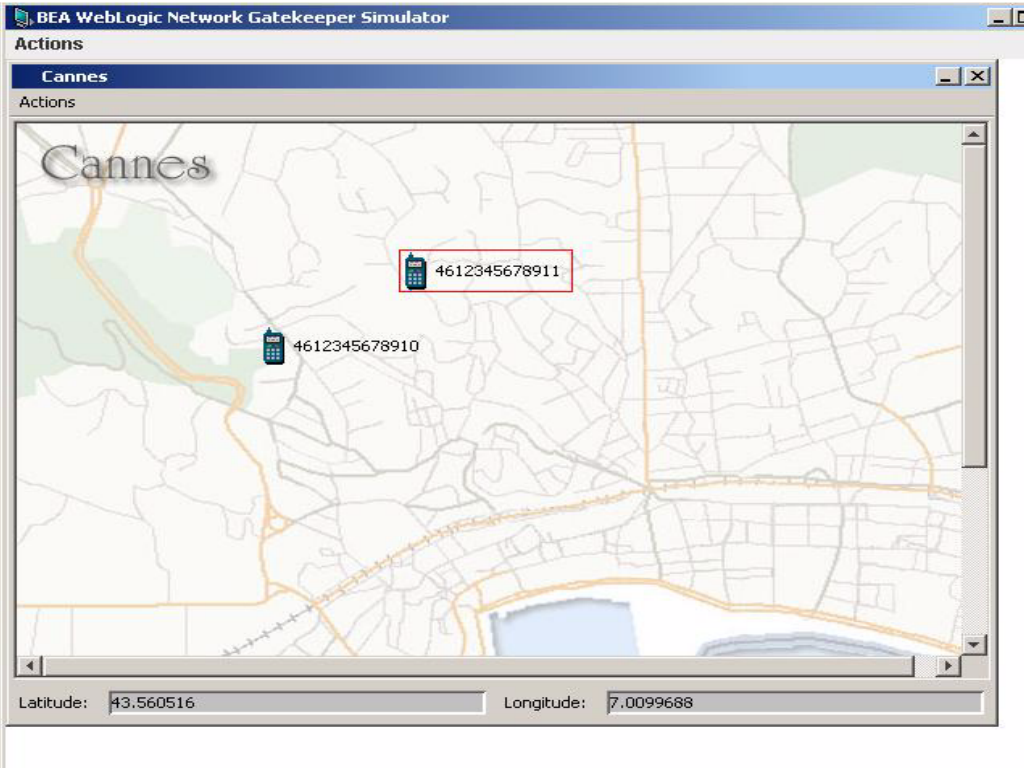
  - applicationLogin
  - applicationLogout
  - changeApplicationPassword
  - getLoginTicketRemainingLifeTime
  - refreshLoginTicket

When an application uses these interfaces, the simulator provides the same behavior as Oracle Communications Services Gatekeeper.

The Oracle Communications Services Gatekeeper Simulator GUI

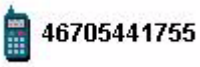
The Oracle Communications Services Gatekeeper Simulator GUI is based on a map. The map can be changed to fit different locations. The GUI is used to add mobile telephony terminals (mobile telephones).

Figure 2-1 Oracle Communications Services Gatekeeper Simulator GUI



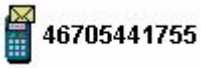
These terminals are given a subscription number. Once the terminal is defined, it can be moved to different locations on the map.

Figure 2-2 Telephone (terminal) icon



The terminals on the GUI can send and receive messages. When a message has arrived at the telephone, an envelope is displayed beside the telephone icon.

Figure 2-3 Telephone (terminal) icon with message



Using mobile terminals

The mobile terminals created in the Oracle Communications Services Gatekeeper Simulator GUI can:

- Show the ID of the phone
- Indicate when messages have arrived
- Be moved using click and drag
- Receive and display SMSes.
- Receive and display PAP messages.
- Receive and display MMSes of the following types:
  - Text: plain text, HTML, and WML text only messages.
  - Graphics: gif, wbmp, tiff, png, and jpeg graphic files.
  - Applications: multipart, multipart-mixed.
- Send SMSes.
- Send MMSes of the following types:
  - Text: plain text, HTML, and WML text only messages.
  - Graphics: gif, wbmp, tiff, png, and jpeg graphic files.
  - Applications: multipart, multipart-mixed, and SMIL.

Note: SMSes and MMSes cannot be sent directly from a terminal to another. When sending a message, the message can be received by an application, but it cannot be sent directly to another phone.

Using the map

The Oracle Communications Services Gatekeeper Simulator GUI can:

- Load new images as maps from any URL, stored locally or on the Internet.
- Set the geographical coordinates of the map.
- Display the coordinates of a selected phone.
- Display several maps simultaneously.

Using utilities

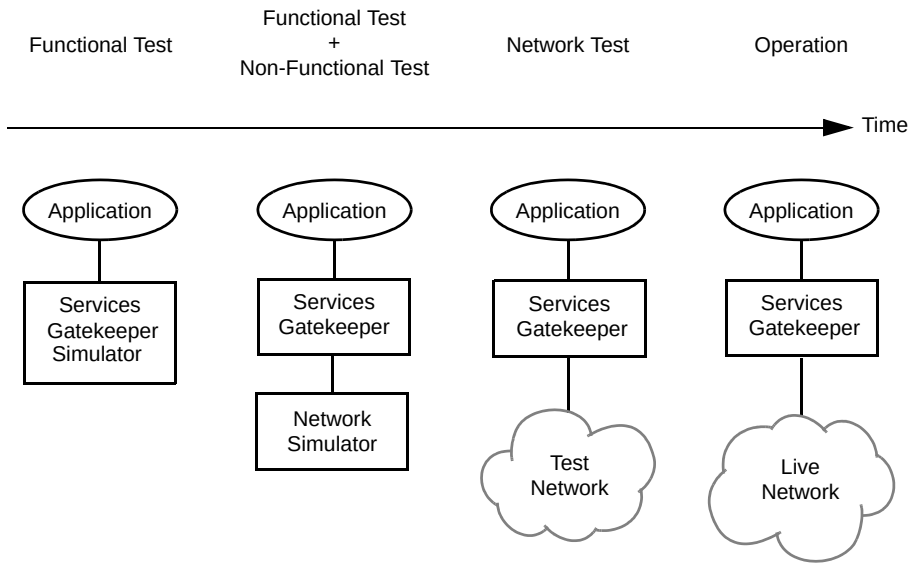
The Oracle Communications Services Gatekeeper Simulator GUI can:

- Save a configuration - the map including coordinates - to file.
- Load a configuration from file.

Test Flow

Figure 2-4 shows the complete Oracle Communications Services Gatekeeper application test flow, from the application developers' functional test to deployment in a live network. An application developer can perform functional tests using Oracle Communications Services Gatekeeper Simulator. The other tests in the flow must be performed in cooperation with a network operator.

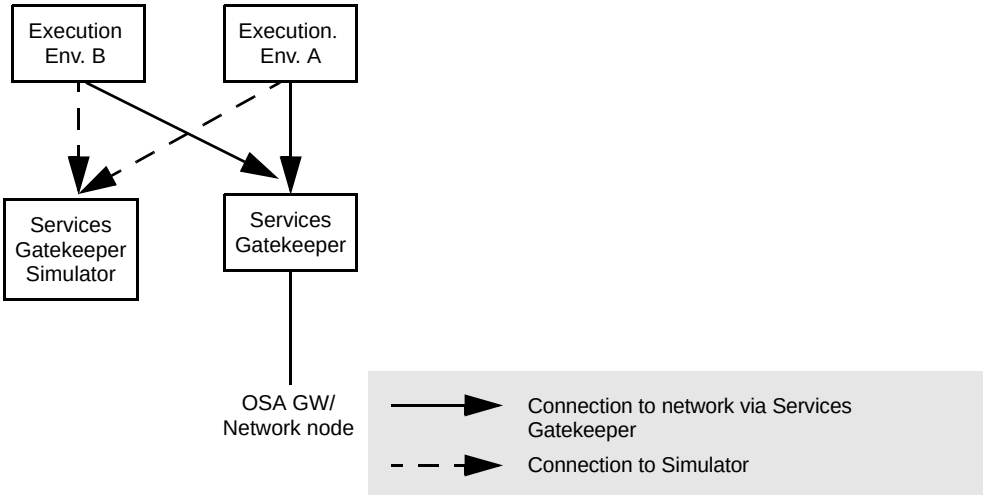
Figure 2-4 Application test flow



An overview of the relationship between Oracle Communications Services Gatekeeper Simulator and Oracle Communications Services Gatekeeper is shown in Figure 2-5.

.

Figure 2-5 Oracle Communications Services Gatekeeper SDK in relation to Oracle Communications Services Gatekeeper



In the first stage of testing, the Web Services endpoints are provided by Oracle Communications Services Gatekeeper Simulator. In production, the application uses endpoints provided by Oracle Communications Services Gatekeeper.

Supported Configurations

The Oracle Communications Services Gatekeeper SDK and Simulator runs on WebLogic Server. It is supported on the following platforms:

Microsoft Windows XP SP2 on x86

Table 2-1 Requirements

Operating System Version and Patches	Windows XP Service Pack 2 and later Service Packs
Chip Architecture and Minimum Processor Speed	x86 and compatible chip architectures (1.3 GHz)
RAM	1 GB minimum, 2 GB recommended

Red Hat Enterprise Linux 4.0 on x86

Table 2-2 Requirements

Operating System Version and Patches	Red Hat Enterprise Linux 4.0-1 AS, ES, WS Kernel 2.6.9-11.ELsmp #1 SMP x86_32 GNU/Linux with glibc 2.3.4-2.9 and later updates and errata levels
Chip Architecture and Minimum Processor Speed	x86 (400 MHz)
RAM	1 GB minimum, 2 GB recommended
Additional	Must support X11

CHAPTER 3

Using the Oracle Communications Services Gatekeeper SDK

The following sections describe how to use the Oracle Communications Services Gatekeeper SDK:

- Start the Oracle Communications Services Gatekeeper Simulator
- Add a new map
- Open a map
- Create user credentials for an application
- Remove a mobile phone/terminal
- Set the location of a mobile phone
- Send an MMS
- Open an MMS
- Send an SMS
- Open an SMS or PAP message
- Register an off-line notification for SMS
- Register an off-line notification for MMS

Start the Oracle Communications Services Gatekeeper Simulator

To start the Oracle Communications Services Gatekeeper Simulator from the Windows Start Menu:

Choose **Oracle Communications Services Gatekeeper SDK**, and then **Start Oracle Communications Services Gatekeeper SDK**.

To start the Oracle Communications Services Gatekeeper Simulator from the command line, enter:

- *$BEA_HOME*`\wlserver_10.3\samples\domains\sdk\bin\startWebLogic` (Windows)
- *$BEA_Home*`/wlserver_10.3/samples/domains/sdk//bin/startWebLogic.sh` (UNIX)

where $*BEA_HOME* is the name of the directory in which you installed the Oracle Communications Services Gatekeeper SDK.

The Oracle Communications Services Gatekeeper SDK Simulator GUI is displayed.

The WebLogic Server Administration console can be used to configure the Oracle Communications Services Gatekeeper SDK simulator and runtime environment. Use a supported web browser to go to `http://<server>:<port>/console` where the `<server>` and port correspond to your Oracle Communications Services Gatekeeper installation. Default values are `localhost` and `7001`.

Add a new map

Starting in the **Oracle Communications Services Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Add Map...**

   This opens the **Add Map** dialogue box.

2. In the **Map name** field, enter a description of the map.

3. In the **Map URL** field, enter the URL to the map, or choose a map located on the file system by clicking Browse and selecting a file.

   Supported map formats are GIF, JPEG, and BMP. The URL can be HTTP or File, for example http://some-map-hosting-company/london.jpg.

4. In the **Upper left corner coordinates** group:

   In the **Latitude field**, enter the latitude of the upper left coordinate of the map. North of the equator is a positive value between 0 and 90. South of the equator is a value between 0 and -90.

   In the **Longitude field**, enter the longitude of the upper left coordinate of the map. West of the Greenwich zero meridian is a negative value between 0 and -180. East of the Greenwich zero meridian is a positive value between 0 and 180.

5. In the **Lower right corner coordinates** group:

   In the **Latitude** field, enter the latitude of the lower right coordinate of the map. North of the equator is a positive value between 0 and 90. South of the equator is a negative value between 0 and -90.

   In the **Longitude** field, enter the longitude of the lower right coordinate of the map. West of the Greenwich zero meridian is a negative value between 0 and -180. East of the Greenwich zero meridian is a positive value between 0 and 180.

6. Click **OK**.

   Now the map and its meta information is stored under the name <Map name>.map in the directory `$DOMAIN_HOME\servers\<Servername>\maps`. This file can be transferred to any other Oracle Communications Services Gatekeeper Simulator.

Open a map

Starting in the **Oracle Communications Services Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Open Map...**

   This opens the **Open map** dialogue box.

2. From the **Map name** drop down list, choose a map to display.

   A preview of the map, together with data on the coordinates of the map, is displayed.

3. Click **OK**.

   This opens the map in the simulator GUI. Repeat this procedure for every map you want to display.

Create user credentials for an application

Starting in the **Oracle Communications Services Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Create User...**

   This opens the **Create User** dialogue box.

2. In the **Application Instance Id** field, enter the user name the application should use when establishing a session (login). Must be unique.

3. In the **Service Provider Id** field, enter the service provider account ID for the application.

4. In the **Application Id** field, enter the application account ID for the application.

5. In the **Password** field, enter the password the application should use when establishing a session (login). The password must be at least 8 characters long.

6. Click **OK**.

   The user credentials are now registered and applications can use these to login.

Remove a mobile phone/terminal

Starting in the <Map name> window:

1. Right click on the telephone to be removed.

2. From the displayed menu, choose **Remove**.

   The telephone is removed.

Set the location of a mobile phone

Starting in the <Map name> window:

1. Click and hold the cursor on the telephone icon using the left mouse button.

2. Drag the telephone on the map.

   The terminal's coordinates are displayed as it is moved.

Send an MMS

This procedure is used for sending Multimedia Messages to an application. Sending messages from one terminal in the Gatekeeper to another is not supported.

Starting in the <Map name> window:

1. Right click on the icon of the telephone from which you wish to send the MMS.

A menu is displayed.

2. From the menu, choose **Send multimedia message....**

   The **Send multimedia message** dialogue box is opened.

3. In the **To** field, enter the service number to which you wish to send the MMS.

4. Click **Add content**.

   In the **Message** group, a row is opened for editing.

5. In the **Type** column, choose the type of content from the selection list.

6. In the **URL** column, enter the URL pointing to the content you wish to add to the message, or choose a file located on the file system by clicking **Browse** and selecting a file.

7. Repeat the above steps for each part of the MMS.

8. To remove any content, select the row containing the part and click **Remove content**

9. Click **Send**.

   The MMS is sent.

Open an MMS

When an MMS arrives at a phone, an envelope symbol appears beside the telephone icon. Follow the instructions below to open the MMS.

Starting in the <Map name> window:

1. Right click on the telephone that has received a new MMS.

   A menu is displayed.

2. From the menu, choose **Read multimedia message....**

   The **Read multimedia message** dialogue box is opened.

   In the left pane, a reference to the new message is displayed. Select the message reference and the content of the MMS is displayed in the right pane.

Send an SMS

This procedure is used for sending Short Messages to an application. Sending messages from one terminal in the Gatekeeper to another is not supported.

Starting in the <Map name> window:

1. Right click on the icon of the telephone from which you wish to send the SMS.

   A menu is displayed.

2. From the menu, choose **Send message....**

   The **Send message** dialogue box is opened.

3. In the **To** field, enter the service number to send the SMS to.

4. In the **Message** field, enter the text to send.

5. Click **Send**.

   The SMS is sent.

Open an SMS or PAP message

When an SMS or PAP message arrives at a phone, an envelope symbol appears beside the telephone. Follow the instructions below to open the SMS or PAP message.

Starting in the <Map name> window:

1. Right click on the telephone that has received a new SMS or PAP message.

   A menu is displayed.

2. From the menu, choose **Read message....**

   The **Read message** dialogue box is opened.

   In the **From** field, the mailbox ID is displayed.

   In the **Message** field, the message is displayed.

Register an off-line notification for SMS

When sending Short Messages from a terminal in the Oracle Communications Services Gatekeeper Simulator, the message is sent to a service activation number. This registers an offline notification for applications that poll for mobile originated short messages. Mobile originating Short Messages sent to the service activation number that match a given criteria do not result in a notification callback to an application. Instead the message is stored in Oracle Communications Services Gatekeeper Simulator.

Starting in the **Oracle Communications Services Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **SMS Notifications...**

   This opens the **SMS Notifications** dialogue box.

2. Click **Add Notification.**

3. In the **Activation Number** field, enter the service activation number. In the **Criteria** field, enter a text to match against to determine if the application should receive the notification. This text is matched against the first word in the message. Leave empty to match all messages.

4. Click **OK**.

The notification is displayed with a registration identifier. The notification can be removed by selecting the notification and then clicking **Remove Notification**.

Register an off-line notification for MMS

When sending Multimedia Messages from a terminal in the Oracle Communications Services Gatekeeper Simulator, the message is sent to a service activation number. This procedure registers an offline notification for applications that poll for mobile originated multimedia messages. Mobile originating Multimedia Messages sent to the service activation number do not result in a notification callback to an application. Instead the message is stored in Oracle Communications Services Gatekeeper Simulator.

Starting in the **Oracle Communications Services Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Enable Received MMS...**

   This opens the **Enable Receive MMS** dialogue box.

2. In the **Activation Number** field, enter the service activation number.

3. Click **OK**.

The notification is displayed with a registration identifier. The notification can be removed by selecting the notification and then clicking **Remove Notification**.

Define session lifetime

When an application establishes a session with Oracle Communications Services Gatekeeper, the session has a lifetime (session ticket lifetime).The default lifetime can be changed.

Starting in the **Oracle Communications Services Gatekeeper Simulator** window:

1. In the **Actions** menu, choose **Session Lifetime...**

This opens the **Session Lifetime** dialogue box.

2. Enter the default lifetime, given in minutes.
3. Click **OK**.

CHAPTER 4

Installing and Configuring the SDK

This chapter describes setting up the Oracle Communications Services Gatekeeper SDK for use. The chapter includes information on:

Installation procedure

To install the Oracle Communications Services Gatekeeper SDK:

Note: The sample domain that is provided with the Oracle Communications Services Gatekeeper SDK can be used directly. Separate domain configuration is unnecessary.

Launch the GUI Installer - Windows

If you are using the GUI-based installer on a Windows machine, do the following:

1. Log in to the Windows system.
2. Go to the directory where you have copied the installation program. You acquire this program either from a Oracle Communications Services Gatekeeper SDK CD or the Download Center.
3. If you are using Explorer to find the file, double-click the installation file, `ocsg_sdk410_win32.exe`
4. If you are using the console window to find the file, enter the following command:

```
ocsg_sdk410_win32
```

Note: You can also include the `-log=full_path_to_log_file` option in the command line to create a verbose installation log. For example:

```
ocsg_sdk410_win32 -log=<full_path>install.log
```

5. Go on to "Respond to the Prompts" on page 4-2

Launch the GUI Installer - UNIX/Linux

If you are using the GUI-based installer on a UNIX/Linux machine, do the following:

1. Log into the target UNIX system
2. Go to the directory where you have copied the installation program. You acquire this program either from the Oracle Communications Services Gatekeeper SDK CD or the Download Center.
3. Launch the installation by entering the following commands:

   ```
   chmod a+x ocsg_sdk410_<appropriate-platform-filename>.bin
   ```

   ```
   ./ocsg_sdk410_<appropriate-platform-filename>.bin
   ```

   Note: You can also include the `-log=full_path_to_log_file` option in the command line to create a verbose installation log. For example:

   ```
   ocsg_sdk410_<appropriate-platform-filename>.bin
   -log=<full_path>install.log
   ```

4. Go on to "Respond to the Prompts" on page 4-2

Respond to the Prompts

The installation program prompts you to enter specific information about your system and configuration. For instructions on responding to the prompts during installation, see the following table.

In this window...	Perform the following action...
Welcome	Click **Next** to proceed with the installation. You may cancel the installation at any time by clicking **Exit**.
Choose BEA Home Directory	Specify the BEA Home directory that will serve as the central support directory for the installed on the target system. If you already have a BEA Home directory on your system, you can select that directory (recommended) or create a new BEA Home directory. **Note:** If you also have Oracle Communications Services Gatekeeper installed on this machine, you will need to select a new BEA home. A separate version of WebLogic Server will be installed just for the SDK. If you choose to create a new directory by typing a new directory name in the BEA Home Directory field, the installation program automatically creates one for you. You can also click **Browse** and select a directory from the **BEA Home Directory Selection** window.
Choose Products and Components	Make sure Oracle Communications Services Gatekeeper SDK is selected. Click **Next**.
Choose JDK	Select the JDK to use. Click **Next**.
Choose Product Installation Directory	Specify the directory in which you want to install the Oracle Communications Services Gatekeeper software. This is the directory from which information will be copied during the domain configuration phase. Once you have chosen your directory, click **Next**. You can accept the default product directory (ocsg_4.1) or create a new product directory.
Install Windows Service	Do not install Node Manager Service. Click **Next**.

In this window...	Perform the following action...
Choose Shortcut Location This window is displayed only under the following conditions: • You have Administrator privileges. • You are performing an initial installation. • You are installing on a Windows platform.	Specify the Start menu folder in which you want the Start menu shortcuts created. You can select from the following options: • **All Users Start menu folder** Selecting this option provides all users registered on the machine with access to the installed software. However, only users with Administrator privileges can create shortcuts in the All Users folder. Therefore, if a user without Administrator privileges uses the Configuration Wizard to create domains, Start menu shortcuts to the domains are not created. In this case, users can manually create shortcuts in their local Start menu folders, if desired. Press ALT+Y on the keyboard to select the All Users Start Menu. • **Local user's Start menu folder** Selecting this option ensures that other users registered on this machine will not have access to the Start menu entries for this installation. Press ALT+N on the keyboard to select the Local User's start menu.
Status	Read the information displayed about Oracle products and services. When the installation program has finished copying the specified files to your system, click **Next**.
Installation Complete	Specify whether you want to run the QuickStart application. QuickStart, designed to assist first-time users in evaluating, learning, and using the software, provides quick access to domain configuration wizard. Clear the check box for this option if you do not want to launch QuickStart. Unless you want to make changes to the standard sample domain, a separate domain configuration is not necessary.

Setting up WS-Policy

One of the first things you must do in setting up Oracle Communications Services Gatekeeper SDK is to establish Web Services security. Web Services security controls Oracle Communications Services Gatekeeper Simulator’s interactions with Application Service Providers

Web Services Security

Web Services Security provides end-to-end message-level security for web services through an implementation of the WS-Security standard. WS-Security defines a mechanism for adding three levels of security to SOAP messages:

- Authentication tokens. WS-Security authentication tokens lets an application provide a user name and password or X509 certificate for the purpose of authentication headers.
- XML encryption. WS-Security's use of W3C's XML encryption standard enables the XML body or portion of it to be encrypted to ensure message confidentiality.
- XML digital signatures. WS-Security's use of W3C's XML digital signatures lets the message be digitally signed to ensure message integrity. The signature is based on the content of the message itself (by applying a hash function and public key), so if the message is altered en route, the signature becomes invalid.

Oracle Communications Services Gatekeeper uses WebLogic Server mechanisms for Web Services security- see:

- *Oracle WebLogic Server Securing WebLogic Web Services* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/webserv_sec/
- *Oracle WebLogic Server Understanding WebLogic Security* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/secintro/
- *Web Services Security specifications* at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Message level security for SOAP messages is achieved by applying WS-Security and WS-Security policy standards. Authentication is handled transparently by WS-Security and subsequently by the configured authentication providers and login modules of the WebLogic Security framework. WS-Security also supports signing and encrypting a message by providing a security token hierarchy associated with the keys used for signing and encryption (for message integrity and confidentiality).

The following steps outline the general WebLogic security configurations that have to be performed, either automatically using a script or manually from the Administration Console.

- Configure Policies for WS-Security as described below.
- If using SAML tokens, configure WebLogic SAML Identity Assertion Provider which authenticates users based on SAML assertions and SAML credential mapping provider. A SAML Identity Assertion Provider is required only if you are using SAML assertions.

Configuration Workflow: Policies for WS-Security

This section outlines how to apply an existing WS-Policy and where to find more information about creating and using custom WS-Policies.

Apply a WS-Policy to a Web Service: Quick start

This section outlines how to apply a WSSE policy to a Web Service endpoint in the Oracle Communications Services Gatekeeper Simulator.

Standard WebLogic Server mechanisms are used. See *Oracle WebLogic Server Management Console On-line Help* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/ConsoleHelp/pagehelp/J2EEwebservicewebservicepolicytitle.html for a full description on how to configure a policy file for a Web Service.

The Oracle Communications Services Gatekeeper Simulator must be started, see Start the Oracle Communications Services Gatekeeper Simulator.

Starting in WebLogic Console:

1. In the **Domain Structure** pane, select **Deployments**.
2. In **Summary of Deployments** page, expand **simulator**.
3. Click on a Web Service to apply Web Services security to, for example **SendSmsService**. All Web Services are named according to the interface they implement.

   This shows the page **Settings for <Web Service>**
4. Click the **Configuration** tab.
5. Click **WS-Policy** sub-tab.
6. Click **Service endpoint <Web Service>**.
7. Choose which security policy to apply for the endpoint:
   a. Select the appropriate WS-Policy file in **Available Endpoint Policies**, see "Available default WS-Policies" on page 4-7.
   b. Move it to the list in **Chosen Endpoint Policies** by clicking on the arrow button.
   c. When the WS-Policy files have been chosen, click **OK**.
8. In the **Save Deployment Plan Assistant** you choose where to store the deployment plan.

9. Apply the changes.

Note: Applying a security policy to a Web Service establishes, by default, both inbound and outbound security policies. Because there is no way for Oracle Communications Services Gatekeeper Simulator to know what security policies may be required by a client to which it is returning a notification, outbound security must be turned off. If you wish to secure the link by which Oracle Communications Services Gatekeeper Simulator returns notifications, you should use SSL.

To turn off outbound security associated with a particular WS-Policy file, you must edit the plan.xml file that is created when you attach Policy to a Web Service, as in step 8 above. Make sure the <value> element is set to `inbound` as in the following stanza:

Listing 4-1 Plan.xml snippet to be edited

```
<variable>
      <name>WsPolicy_policy:Auth.xml_Direction_11745107731400</name>
      <value>inbound</value>
</variable>
```

Create and Use a Custom WS-Policy

See *Oracle WebLogic Server Securing WebLogic Web Services* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/webserv_sec/ for information on how to create and use a custom WS-Policy file.

Also see *Oracle WebLogic Server Management Console On-line Help* at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/ConsoleHelp/pagehelp/J2EEwebservicewebservicepolicytitle.html for a full description on how to configure a policy file for a Web Service

Available default WS-Policies

WS-Policy files can be used to require applications clients to authenticate, digitally encrypt, or digitally sign SOAP messages. Out-of-the-box Oracle Communications Services Gatekeeper supplies files to do those three things, respectively: auth.xml, encrypt.xml, and sign.xml. If the built-in WS-Policy files do not meet your security needs, you can build custom policies.

WS-Policy assertions are used to specify a Web Services' requirements for digital signatures and encryption, along with the security algorithms and authentication mechanisms that it requires, for example Policy for SAML.

CHAPTER 5

Workshop Controls with Oracle Communications Services Gatekeeper

To aid those developers using Workshop for WebLogic Platform™ as their development environment, the Oracle Communications Services Gatekeeper SDK includes a set of custom controls for use in creating clients for Oracle Communications Services Gatekeeper. These controls implement the code needed to access the Web Services interfaces supported by the communication services Oracle Communications Services Gatekeeper provides out-of-the-box and also include support for getting and setting endpoints, getting and using session IDs (for session-based installations), adding attachments, and managing WS-Security Username-Token mechanisms.

Note: If you are a first time user of Workshop, you may wish to look through the Workshop documentation before reading here to get an idea of how Workshop works. The documents include overview material, tutorials, and other related information. The chapter that covers using controls can be found at http://download.oracle.com/cd/E13224_01/wlw/docs100/guide/controls/navBeehiveControls.html. You can also open up the complete set of documentation by clicking **Help** ->**Help Contents** in the Workshop main menu bar. The locally stored help files will open up in your browser. Click on the **Workshop for WebLogic Platform User's Guide** in the left navigation bar and select **Controls**.

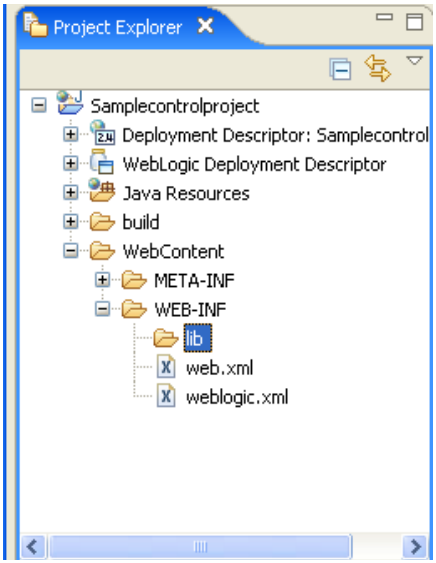
Using the Controls

The Workshop controls for Oracle Communications Services Gatekeeper are packaged as a .jar file (`com.bea.wlcp.wlng.controls.4.1.0.0.jar`) that is located in the `$BEA_HOME/wlserver_10.3/samples/domains/sdk/controls` directory. Complete

JavaDoc for the Controls can be found in `$BEA_HOME/wlserver_10.3/samples/domains/sdk/controls`. To use the Controls:

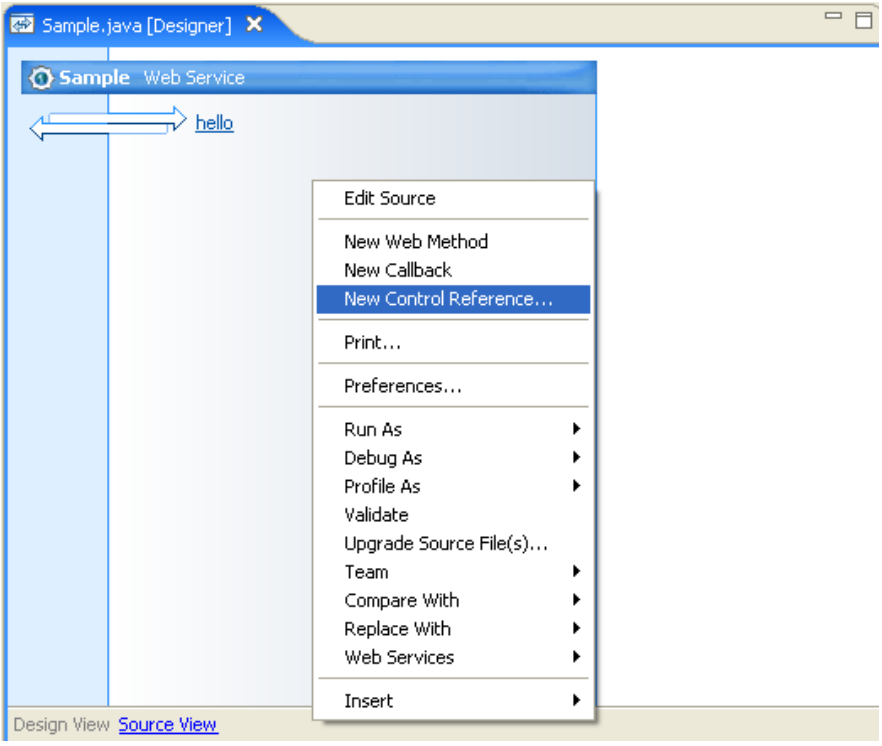
1. Create a Web Services project in Workshop.
2. Drag and drop the .jar file into the `WEB_INF/lib` directory of the project. Workshop will recognize it and register it automatically.

Figure 5-1 Drop the .jar file in WEB_INF/lib



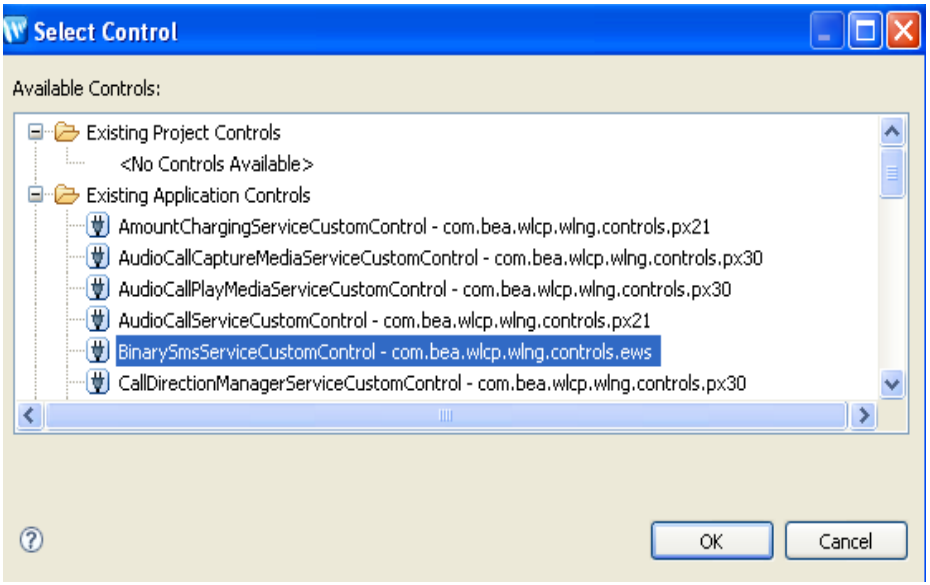
3. Create a New WebLogic Web Service.
4. Right click in the **Design** view and select **New Control Reference**.

Figure 5-2 Select New Control Reference



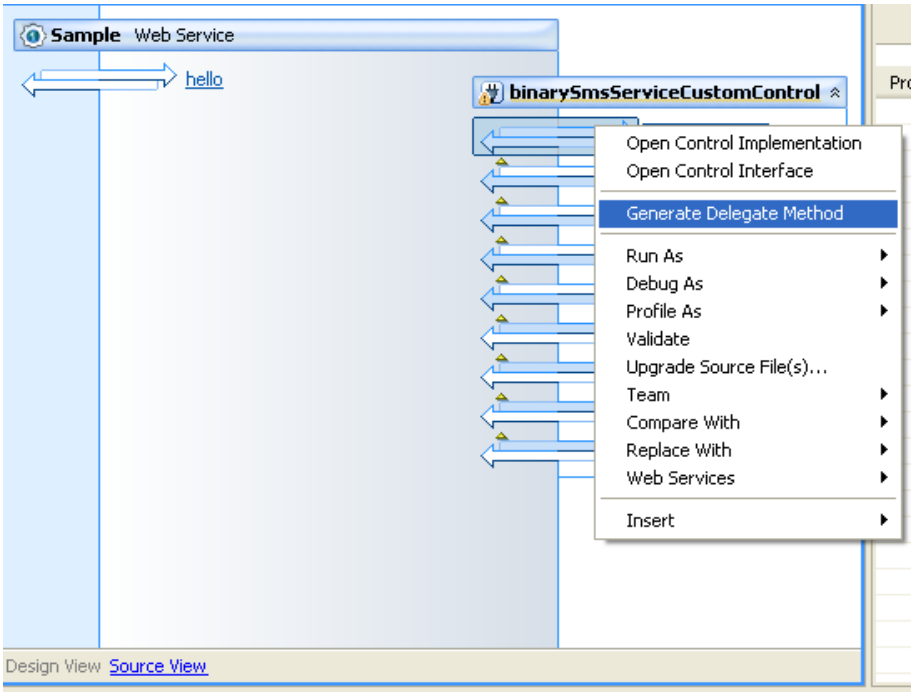
5. From the Select Control dialog box, chose the control you are interested in using.

Figure 5-3 Select Control



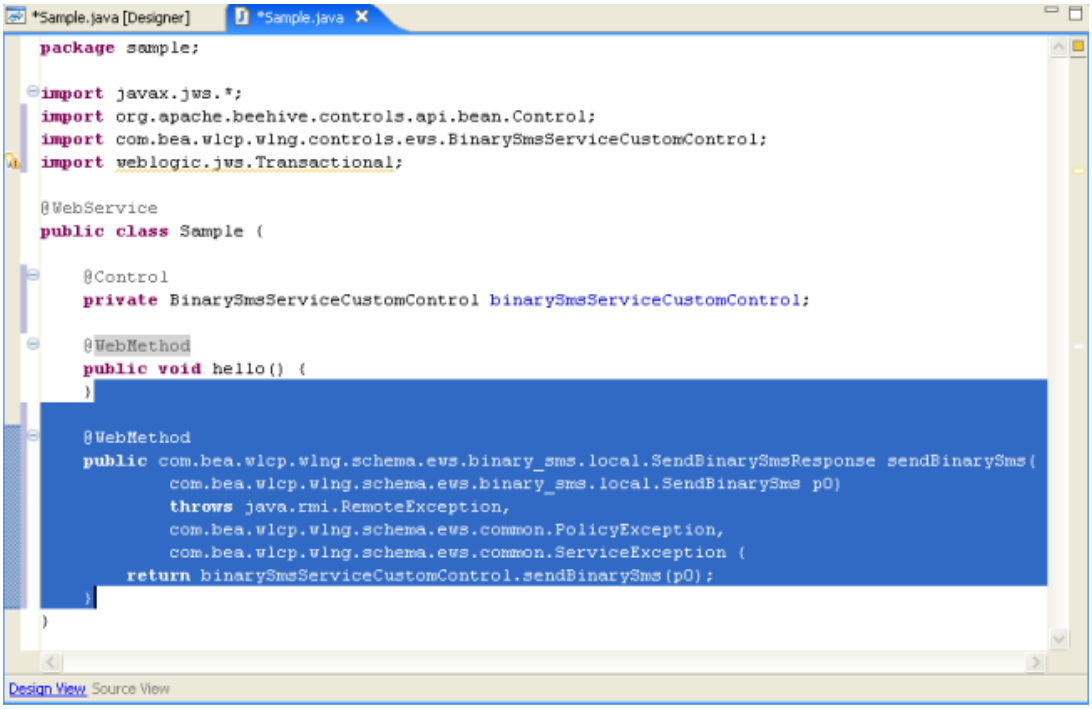
6. Once the control has been added, right click on the method you wish to use, and select **Generate Delegate Method**.

Figure 5-4 Generate Delegate Method



7. The method is inserted in your source code.

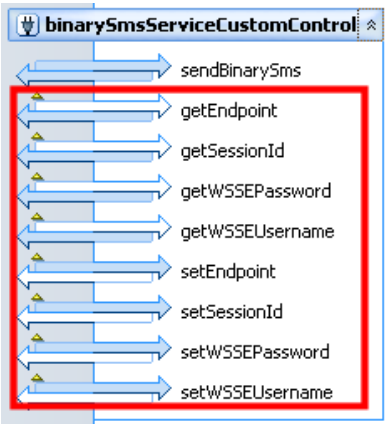
Figure 5-5 Method is inserted



Using the Utility Methods

In addition to the communication service interface methods that are provided by the control, a set of utility methods are also provided. The group includes methods to get and set Web Service endpoints, get and set Session IDs (for session-based installations), get and set WS-Security Username and Password, get and set Attachments for those interfaces that support them. You add these methods to your code in the same way as you add the main interface methods. Mechanisms internal to the controls take care of managing the methods' use.

Figure 5-6 Utility Methods for Binary SMS(in red)



Method Signatures for Utility Methods

Endpoints

- `public void setEndpoint(String url);`
- `public String getEndpoint();`

Session IDs

- `public void setSessionId(String id);`
- `public String getSessionId();`

Attachments

- `public void setAttachment(byte[] content, String contentType);`
- `public byte[] getContent();`
- `public String getContentType();`

Username Tokens

- `public void setWSSEUsername(String username);`
- `public String getWSSEUsername();`

- `public void setWSSEPassword(String passwd);`
- `public String getWSSEPassword();`

For more information on what these utility methods are managing for you, see the "Interacting with Oracle Communications Services Gatekeeper" chapter in the *Application Development Guide*, a separate document in this set.