Oracle® Communications Services Gatekeeper

OAuth Guide

Release 5.1

E37521-01

June 2013

ORACLE®

Oracle Communications Services Gatekeeper OAuth Guide, Release 5.1

E37521-01

Contents

3 Monitoring OAuth Services in Service Gatekeeper

4 Developing Services Gatekeeper Services Using OAuth

Preface

This guide explains how to use the Open Authorization Protocol (OAuth) features with Oracle® Communications Services Gatekeeper (Services Gatekeeper).

Audience

This document is intended for developers who create applications for use with Oracle Communications Services Gatekeeper that allow access to protected resources.

This includes:

- Third-party application developers who want to integrate telephony-based functionality into their products
- Operator-based system developers who want to extend the functionality of Oracle Communications Services Gatekeeper or to integrate it with Partner Relationship Management (PRM) or Operations Support Systems (OSS) tools

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 Services Gatekeeper documentation:

- *Oracle Communications Services Gatekeeper Application Developer's Guide*
- *Oracle Communications Services Gatekeeper Communication Service Guide*
- *Oracle Communications Services Gatekeeper Concepts Guide*
- *Oracle Communications Services Gatekeeper OAM Java API Reference*
- *Oracle Communications Services Gatekeeper One API Application Developer's Guide*
- *Oracle Communications Services Gatekeeper Platform Test Environment Guide*

- *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*
- *Oracle Communications Services Gatekeeper SDK User's Guide*

1

Using OAuth With Services Gatekeeper

This chapter provides an overview of how Oracle Communications Services Gatekeeper (Services Gatekeeper) uses the Open Authorization Protocol (OAuth) to protect resources.

OAuth 2.0 is an open source Web authorization protocol developed by the Internet Engineering Task Force (IETF). For detailed specifications and more information see:

`http://tools.ietf.org/html/rfc6749`

About Services Gatekeeper Support for OAuth Authentication Server

The Services Gatekeeper OAuth implementation allows service providers to offer authorized third-party application access to protected resource owner resources over HTTP.

OAuth is an additional layer of security, in addition to the SLAs and policy control security features that Services Gatekeeper already offers. These security features all work together.

An application `instanceId` defined in Services Gatekeeper can be mapped to a `client_id` defined in the OAuth specification, seamlessly integrating regular SLA functionality. Because OAuth is enforced as a security mechanism, OAuth security is enforced before a Services Gatekeeper SLA.

For more information on supported communication services, see the *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*.

The OAuth2.0 security mechanism can only be enforced for REST-based APIs deployed on Services Gatekeeper. It is not possible to protect the SOAP APIs using OAuth. Services Gatekeeper protects the communication services listed in "Supported Communication Services" as well as any custom APIs that you deploy.

OAuth 2.0 security supports Transport Layer Security (TLS) if required by a client. See "OAuth Configuration" for the required configuration setting.

Understanding OAuth 2.0 Concepts

OAuth is an open standard for authorization. It allows users (your subscribers) to share their private resources with a third party without having to provide their own security credentials. These resources could be photos, videos, contact lists, location and billing capability, and so on, and are usually stored with another service provider. For example, photos stored on a dedicated photo Web storage site.

OAuth does this by granting requesting (client) applications a token, once access is approved by the resource owner. Each token grants access to a specific resource for a

specific period. The requesting application uses the token for access to resources stored with another service provider, instead of the owner's credentials.

A resource can be:

- A single file such as a photo or video.
- Access to a Web site, such as the services of a video editing Web site.
- Personal information such as their location or billing capability.

Understanding OAuth Terminology

Table 1–1 lists OAuth terminology and definitions.

Table 1–1 OAuth Terminology and Definitions

Term	Definition
OAuth	Open Authorization Protocol
resource	The Web resource protected by OAuth Protocol.
resource owner	An entity capable of granting access to a protected resource. In the operator context this is defined as Resource owner URI (tel: or sip:)
Application Client	An application making protected resource requests on behalf of the resource owner and with the resource owner's authorization. The term client does not imply any particular implementation characteristics (for example, whether the application executes on a server, a desktop, or other devices).
scopeId	Unique string that identifies a resource and used as part of scope-token by application client.
Protocol Endpoint	Network URI representing the location of a service to: ■ obtain an authorization code and other values ■ obtain an access token ■ submit a grant. ■ access a resource
Client Identifier	A unique string representing the registration information provided by the client.
authorization grant	Represents the authorization given by the resource owner to a client application. An authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.
Access Token	Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client.
Refresh Token	Refresh tokens are credentials used to re-obtain access tokens.
Authorization Server	Server that issues authorization codes and access token.
Resource Server	Server that hosts protected resources and validates access token during resource access.
Authorization Endpoint	Used to obtain authorization from the resource owner using user-agent redirection.

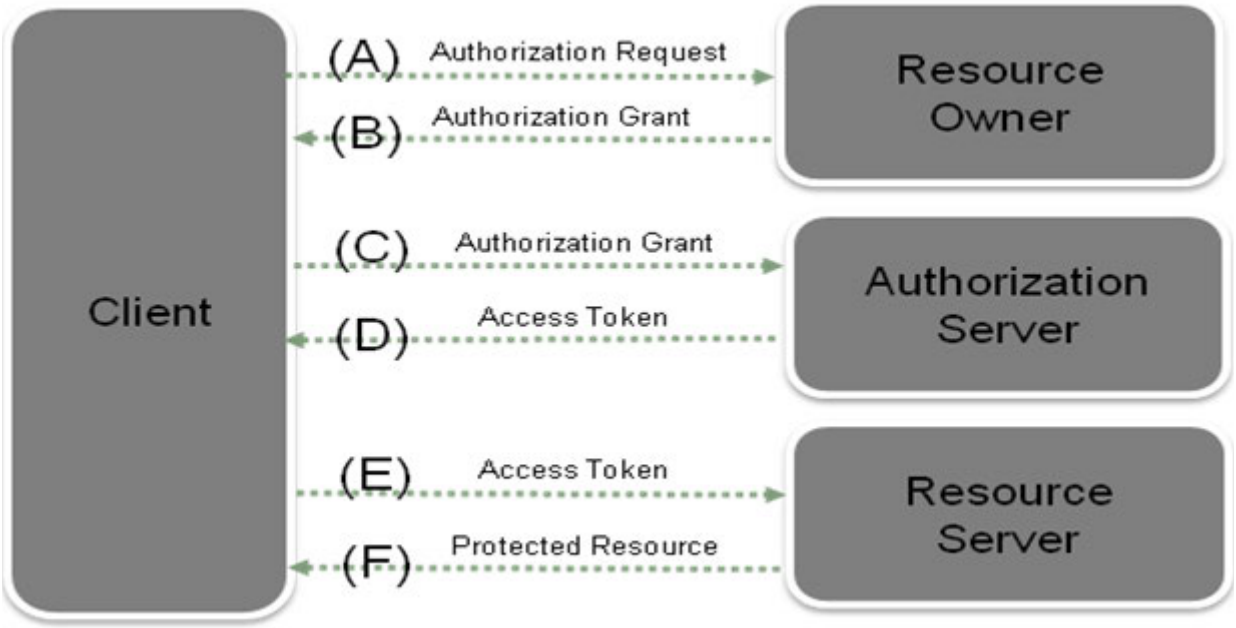
Table 1–1 (Cont.) OAuth Terminology and Definitions

Term	Definition
grant endpoint	URI supported by Services Gatekeeper to post the authentication result to issue the authorization code (defined by Services Gatekeeper).
Redirection Endpoint	After completing its interaction with the resource owner, the Authorization Server directs the resource owner's user-agent back to the client. The Authorization Server redirects the user-agent to the client's redirection endpoint previously established with the Authorization Server during the client registration process or when making the authorization request.
Authentication Server	Server that validates resource owner identity (defined by Services Gatekeeper).
Delegated Authentication	Authentication mode supported by Services Gatekeeper to integrate with 3rd party authentication systems.
Subscriber Manager	Component in Services Gatekeeper to validate subscribers provisioned in Services Gatekeeper database.
Custom Subscriber Manager	Component that authenticates resource owner's username and password with a custom identity store (such as LDAP).
Group URI	URI that represents a group of Resource Owners.
Group Owner	Owner of the Group URI. Issues authorization token on behalf of the group members.
applicationInstanceID	String that uniquely identifies the ApplicationInstance. One applicationInstanceId can be mapped with one OAuth2 Client Identifier, so that SLA can be proceed for OAuth2 based traffic.

About the OAuth/Services Gatekeeper Entities and Their Relationships

Figure 1–1 shows an example OAuth protocol flow for a resource access request:

Figure 1–1 OAuth Flow and Entity Relationships



(A) The client requests authorization from the resource owner. The authorization request can be made directly to the resource owner (as shown), or preferably indirectly using the Authorization Server as an intermediary.
(B) The client receives an authorization grant, including a credential representing the resource owner's authorization, expressed using one of four grant types defined in this specification or using an Extension grant type. The authorization grant type depends on the method used by the client to request authorization and the types supported by the Authorization Server.
(C) The client requests an access token by authenticating with the Authorization Server and presenting the authorization grant.
(D) The Authorization Server authenticates the client and validates the authorization grant, and if valid issues an access token.
(E) The client requests the protected resource from the resource server and authenticates by resending the access token.
(F) The resource server validates the access token, and if valid, serves the request.

About the OAuth Protocol Endpoints

The OAuth2.0 specification defines three types of protocol endpoints.

- **Redirection Endpoint**: The redirection endpoint is a URI used by Authorization Server to return authorization credentials responses from the Authorization Server to the client using the resource owner user-agent.
- **Authorization Endpoint**: The authorization endpoint interacts with the resource owner (typically the subscriber) and obtain an authorization grant which will be issued to an application client by the resource owner. The Authorization Server must first verify the identity of the resource owner before granting the authorization grant. This authorization grant will be exchanged by the application client for an access token.
- **Token Endpoint**: The client uses the token endpoint to obtain an access token by presenting its authorization grant (the authorization code) or refresh token. The token endpoint is used with every authorization grant except for the implicit grant type (since an access token is issued directly).

Understanding How Services Gatekeeper Works with OAuth

This section explains how the Services Gatekeeper functionality is mapped to the OAuth specification.

OAuth Component to Services Gatekeeper Component Mapping

OAuth defines the following terms that map to the Services Gatekeeper concepts listed:

- **resource**: Defined by the OAuth2.0 specification. In Services Gatekeeper, a resource maps to the API(s) and methods protected by the OAuth token. This is a combination of communication service application-facing interface (Plug-in) name, method name, token expire period, parameters and subResource. resource uniquely identified by scopeId.

  For more information, see "Resource Mapping".

- **scope** request parameter: Defined by the OAuth2.0 specification. Determines the limits of an OAuth token. A scope parameter defining these limits is submitted as part of obtaining an authorization grant.

The format of the scope is defined in the OAuth 2.0 specification as:

```
scope = scope-token *(SP scope-token)

scope-token = 1*(%x21 / %x23-5B / %x5D-7E)
```

Services Gatekeeper maps the scope-token parameter to:

<scopeId>[?<*param*>=<*value*>[&<param>=<*value*>]*]+

Where:

scopeId identifies a resource.

param is a custom parameter defined as part of resource.

value is the value for the resource.

Parameter values submitted as part of the scope can be interpreted by custom interceptors.

For example:

```
scope=chargeAmount?MaxAmount=5&itemId=123SPgetLocation?Accuracy=5
where
SP=blank space
```

- **scopeId**: A unique identifier that represents an OAuth resource during resource mapping and determines the access scope of a resource during an authorization grant.

  Defined as part of mapping a communication service method as an OAuth resource, scopeId is used as the value of the id attribute of the resource tag. Each resource is indicated as owned by a resource owner by creating an association between the resource owner (subscriber URI) and the scopeId. The scopeId is submitted as part of scope-token parameter within the authorization grant request.

  For example:

  1. As part of resource configuration, the oracle.Services Gatekeeper.parlayrest.plugin.PaymentPlugin (communication service) method amountTransaction is created as a resource with scopeId chargeAmount:

     ```
     <resource id="chargeAmount" name="Charge or refund"
     interfaceName="oracle.Services Gatekeeper.parlayrest.plugin.PaymentPlugin"
     methodName="amountTransaction"
     tokenExpirePeriod="3600">
     <parameter name="code" description="billable item id"/>
     </resource>
     ```

  2. The chargeAmount resource is mapped to tel:1234 as the resourceOwner.
  3. During the authorization grant, the application sends scope=chargeAmount as part of the authorization request.

- **resource owner**: Defined by the OAuth2.0 specification. Represented as the target address used in the REST API (communication service), and typically represented as one MSISDN. The MSISDN serves as the connection between the resource defined during configuration time and the resource protected during resource authorization and access time.

  – The resource owner (MSISDN) and the scopeId (collection of resources) are mapped during configuration time.

  - Depending on the grant type, the OAuth authorization code/access token is issued by the resource owner (MSISDN).

- **subResource**: A subResource protects and authorizes multiple resources (API methods) with a single token. Resources can have one or more subResources defined as part of resource definition. Authorization grants to a resource also applies to its subResources.

  For example, for a payment communication service, a resource called **amountTransaction** can be created for charging transactions. A subResource called **checkTransactionStatus** is a method used to query the status of a charging transaction. When a resource owner issues a token for resource **amountTransaction**, it can be automatically used against the **checkTransactionStatus** subResource as well.

- **Application Client:** You map a Services Gatekeeper Application Instance Id to an OAuth application client ID during client creation with the **OAuthclientMBean**. See "Client Management" for details.

Services Gatekeeper relies on the authentication endpoint to validate the resource owner. In the Services Gatekeeper default implementation of the authentication endpoint, the validation will be handled by the Subscriber Manager. See "Resource Owner - Resource Mapping" for more information.

Understanding the OAuth Endpoints

Service Gatekeeper supports the standard endpoints defined in the OAuth specification.

OAuth generates these endpoints that Services Gatekeeper uses:

- **Redirection endpoint**: Provided by an application client during the authorization grant.
- **Authorization endpoint**: The default authorization endpoint is configured to the following URL:

  `https://`*`OCSG_server_IP:port`*`/oauth2/authorize`

- **Token endpoint**: By default, the token endpoint is configured to the following URL:

  `https://`*`OCSG_server_IP:port`*`/oauth2/token`

In addition to the standard endpoints, Services Gatekeeper supports two custom endpoints to facilitate integration with external/custom Authentication Servers:

- **Authentication Endpoint:** Verifies the identity of a resource owner. The authentication endpoint is an extension point offered by Services Gatekeeper handling resource owner authentication and authorization grant collection.

  This endpoint interacts with a resource owner, assuring that the subscriber's identity is valid and providing necessary information for the resource owner to authorize an application to obtain an authorization grant.

  By default, the authentication endpoint uses the following URL:

  `https://`*`OCSG_server_IP:port`*`/oauth2/auth.jsp`

  This URL can be updated by editing the following MBean property:

  OauthService.OauthCommonMBean.AuthenticationURL

- **Grant Endpoint:** The Call back URI supported by Services Gatekeeper to process the successfully authenticated requests and issue authorization grants to application clients.

  After a resource owner grants access to protected resources through authentication, the authorization request is submitted to the grant endpoint, which sends the resource requester to a redirect URI provided by the application along with the authorization code.

  By default, the grant endpoint uses the following URL:

  `https://`*OCSG_server_IP*`:`*port*`/oauth2/grant`

  This URL can be updated by editing the following MBean property:

  OauthService.OauthCommonMBean.GrantURL

For more information about the interactions between these endpoints, see "Implementing a Third-Party Authentication Service"

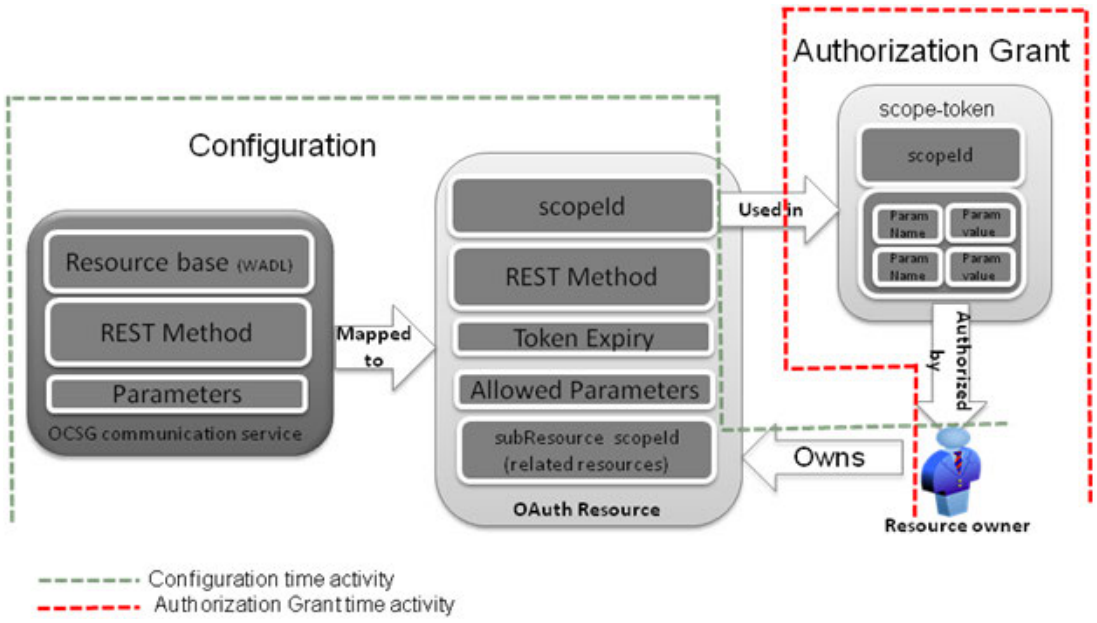
Mapping a Resource to a Services Gatekeeper Method

You can use OAuth2.0 token based security to protect any RESTful communication service, including a customized communication service method, if the specified method is configured as a protected resource.

Figure 1–2 illustrates the relationship between:

- Communication service and an OAuth resource
- Resource and resource owner
- Scope and the resource

Figure 1–2 OAuth Service and Resource Entities Relationships



The communication service-to-resource mapping is explained in detail in "Resource Management".

The scope (defined in the OAuth specification) consists of one or more scope-tokens. Each scope-token contains a `scopeId` (which identifies the resource) and a list of parameter name-values pairs associated with this `scopeId`. The scope is submitted as part of the authorization grant request. The `scopeId`, submitted as part of the scope-token, is interpreted and enforced by the default Services Gatekeeper OAuth interceptor. By default the OAuth interceptor allows all resources to pass. You can also filter these resources to meet the needs of your implementation. If the OAuth interceptor does not meet your implementations's needs, you can replace it with a custom interceptor. For details on modifying the OAuth interceptor or creating a custom interceptor see *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*.

See "OAuth Component to Services Gatekeeper Component Mapping" for more details on the `scope`.

Securing Resources with Multiple Owners

Some APIs require authorization from multiple resource owners. For example:

A Sales Manager may want to expose the location of his sales associates to a location tracking application. This use case requires using the `getGroupLocation` method in the Location API with multiple resource owner addresses.

With Services Gatekeeper, you can create a group of resource owners and associate them with a group URI. You then create a group owner to issue an authorization grant on behalf of the group members. The group owner is represented by an `address` (Group URI), `loginId` and `password` much like a resource owner. The authorization grant issued by a group owner can be easily used with APIs that accept the URIs of group members as one of the request parameters.

The relationships between resources, resource owner(s), groups, group URI and group owner are illustrated in Figure 1–3:

Figure 1–3 Resource and Group Relationships

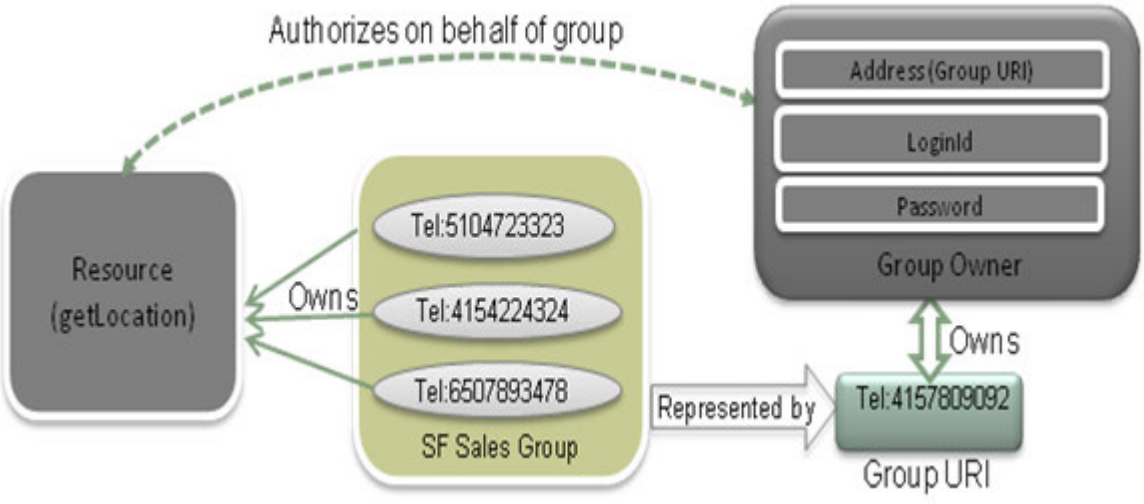


Figure 1–3 show Tel: URIs, but you can also use SIP: URIs.

Use these general steps to protect an API that takes group URIs:

1. Create a group with a group URI using the Parlay X 3.0 `AddressListManagement`.

2. Add members to the group using the Parlay X 3.0 `AddressListManagement`.
3. Create a group owner related to this group URI and password for the group owner.
4. Communicate the group URI and password to a group owner (outside the scope of Services Gatekeeper).
5. The group owner issues an authorization grant to an application to use the member URI as part of API method that requires multiple URIs.
6. Subscribers access the resource (invoking an API method) that accepts multiple resource owners as method parameters.

The default Subscriber Manager supports a mechanism to provision the group owner represented by the group URI. Services Gatekeeper supports this requirement by using the Parlay X 3.0 `AddressListManagement` communication service to create groups. See this specification for more information about address list management: http://www.3gpp.org/ftp/specs/archive/29_series/29.199-13/29199-13-702.zip.

Compliance

This section describes Services Gatekeeper compliance with the OAuth 2.0 specification.

Supported Communication Services

The OAuth2.0 security mechanism can be used with the REST-based communication services provided with Services Gatekeeper, and any custom REST-based API that you deploy. These REST-based communication services are provided by default:

- OneAPI (REST)
- Anonmyous Customer References (ACRs)
- SMS
- MMS
- Location
- Payment

For more information on supported communication services, see the *Oracle Communications Service Gatekeeper RESTful Application Developer's Guide*.

Supported OAuth Server Roles

By default, Services Gatekeeper supports the following OAuth server roles:

- Authorization Server: Issuing authorization grant and access tokens
- Resource Server: Protecting resources and enforcing OAuth token-based access to resources.

Supported Authorization Grant Types

An authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.

By default, Services Gatekeeper supports the following grant types:

- Authorization Code Grant

- Implicit Grant

Extension Grant Flows Enabled Through Supported Grant Types

Services Gatekeeper facilitates customization of the authorization flow by supporting the custom Endpoints described in "Understanding the OAuth Endpoints".

Instead of authenticating with the default Subscriber Manager, it is possible to define a custom authentication URL that authenticates and obtains user's consent and posts the authorization result back to Services Gatekeeper to issue the authorization code.

This delegated authentication is only supported with the authorization code grant type.

See "Implementing a Third-Party Authentication Service" for more information.

Supported Token Types

Services Gatekeeper supports the following token types defined in OAuth2 specification:

- **Bearer**
- **MAC**

Supported Client Profiles

Services Gatekeeper supports Web-based, user-agent-based, and native application profiles.

OAuth Flows Supported by Services Gatekeeper

The following sections illustrate the OAuth authorization grant flows that Services Gatekeeper supports:

- Authorization Code Grant
- Implicit Grant
- Refresh Token Grant

Authorization Code Grant

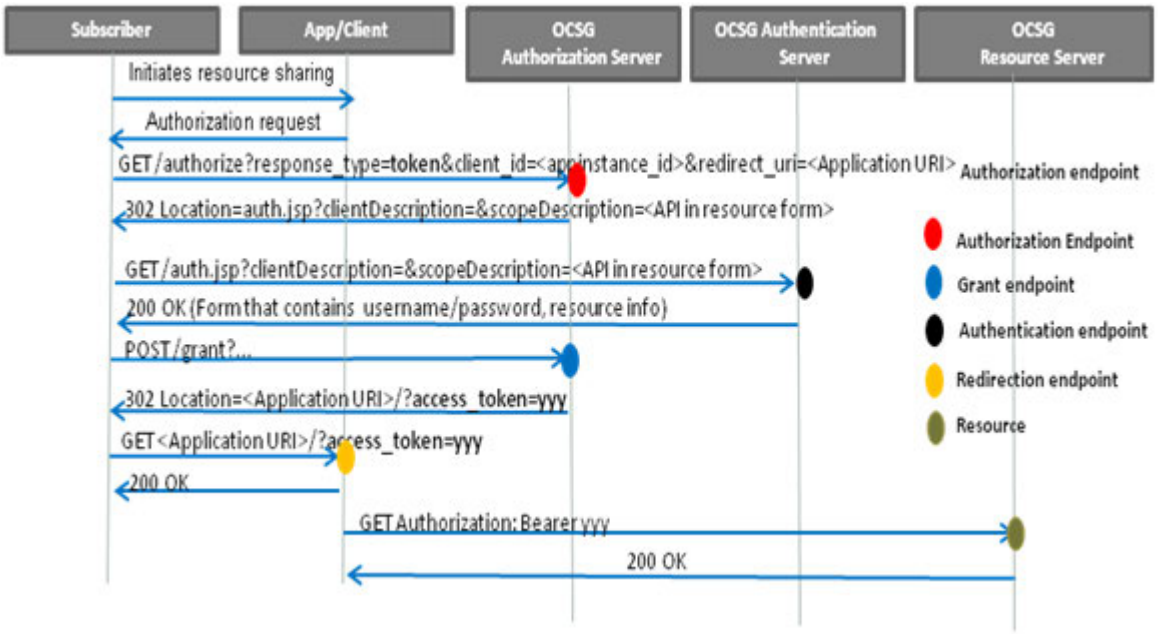
Figure 1–4 shows an OAuth authorization code grant sequence flow diagram.

Figure 1–4 Authorization Code Grant

Implicit Grant

Figure 1–5 shows an Oauth implicit grant sequence flow diagram.

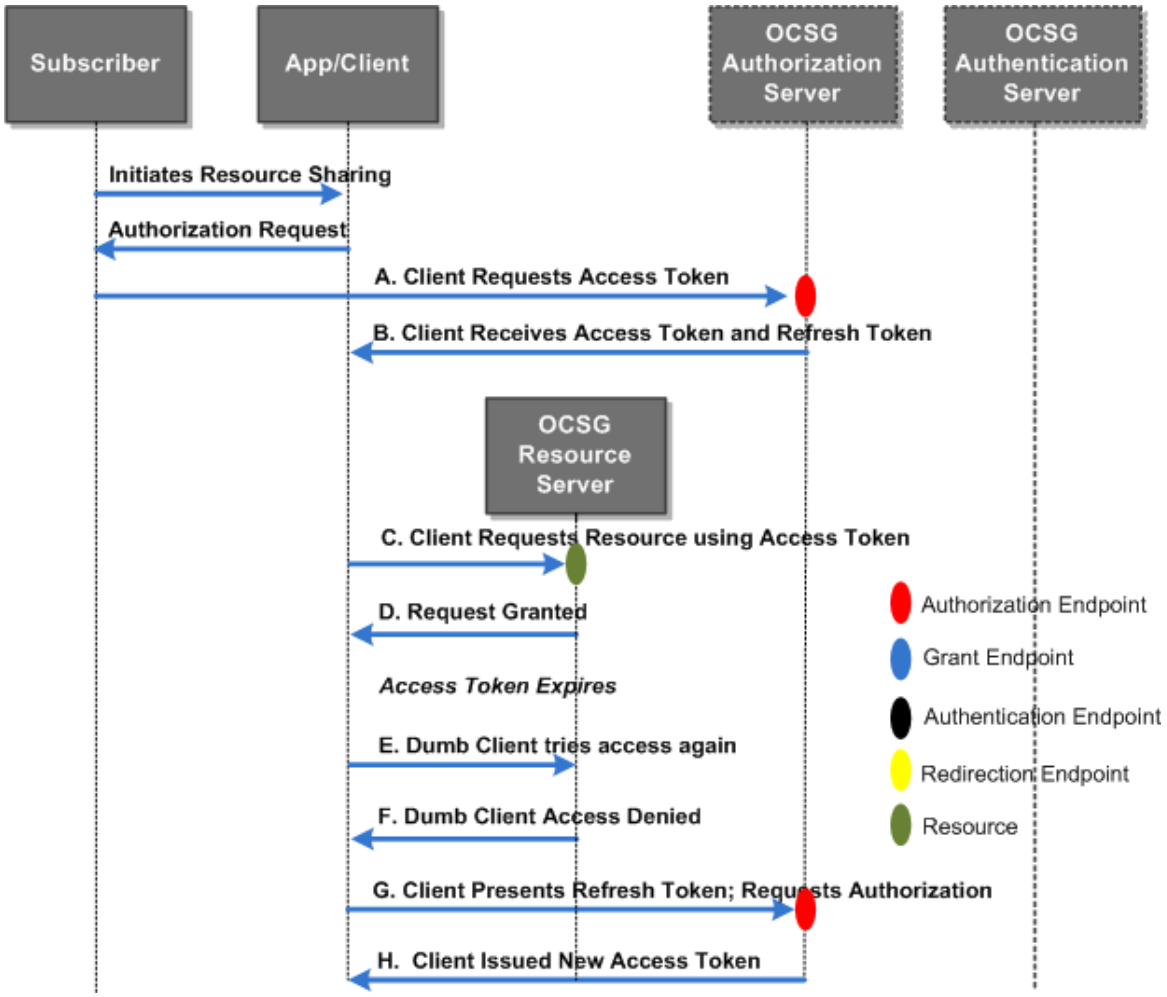
Figure 1–5 Implicit Grant



Refresh Token Grant

Figure 1–6 shows a refresh token grant flow diagram. If the client has way of recognizing when the access token expires (smart client), it skips steps E and F in this diagram. Clients without this knowledge (dumb clients) execute steps E and F.

Figure 1–6 RefreshToken Grant



Supported URIs (Subscribers)

Services Gatekeeper supports the following resource owner URIs for use with OAuth:

- tel: URI (as described in RFC 2806)
- sip: URI (as described in RFC3261)

2

Protecting Services Gatekeeper Resources with OAuth

This chapter explains how to protect Oracle Communications Services Gatekeeper (Services Gatekeeper) resources with the Open Authorization Protocol (OAuth). It starts with information you need to understand about the OAuth technology, then explains the deployment procedure, and finally lists some examples to help you understand the process.

Resource Management

This section describes OAuth resource management as supported by Services Gatekeeper.

Resource Mapping

You can use OAuth to protect a communication services by mapping that communication services to an OAuth resource.

In order to protect an API with OAuth, you model the API method as an OAuth resource, one API to one resource. Resource mapping involves creating a unique `scopeId` to represent the resource, and then mapping it to the API and method names.

You can also define additional context parameters for the resource to use as targets for custom interceptors. These parameters may or may not map directly to the API method parameters.

You can create multiple resources for a single communication service. In this case, resources are aggregated and defined as XML elements in a single XML file. The `scopeId` defined in this XML file is used as part of the `scope` submitted during an authorization grant request. Created resources need to be mapped to the resource owners (identified by subscriber tel:/sip: URIs). resource owners then issue authorization grants to the `scopeIds` (resources) that they own.

See "Understanding the OAuth Resource Format" for details on the resource format and a resource example.

Services Gatekeeper Resource Server

As an OAuth Resource Server, Services Gatekeeper manages the protected resources contained within a service provider's network and accepts and responds to third-party application requests for access to protected resources.

In Services Gatekeeper, a resource is considered a method of a communication service. Resources have subresources that further define specific methods. Authorization

grants to a resource also apply to its subresources. For example, for a payment communication service, a resource called **amountTransaction** can be created for charging transactions. A subresource called **checkTransactionStatus** is a method used to query the status of a charging transaction.

Services Gatekeeper Authorization Server

As an OAuth Authorization Server, Services Gatekeeper obtains a subscriber's permission for access to protected resources when an application makes a request. Services Gatekeeper issues a token to the client application, which is used to access protected resources without requiring the resource owner to provide actual credentials.

When a client application requests access to a protected resource, the Services Gatekeeper REST handler initially checks the request, ensuring that the body contains the needed authorization information. If the request is valid, Services Gatekeeper forwards the request onto the proper communication service. An OAuth interceptor verifies that the token contained in the request is valid before completing the request. Services Gatekeeper then sends a response back to the client application.

Services Gatekeeper Authentication Server

As an Authentication Server, Services Gatekeeper maintains a subscriber database used to store the owners of protected resources. OAuth 2.0 resource owners in Services Gatekeeper must be setup as subscribers in the Authentication Server first. The Authentication Server is used to authenticate subscribers, as resource owners, before initiating authorization to protected resources.

The included Authentication Server is intended for OAuth 2.0 demonstration and development purposes.

Provisioning Mapped Resources

Services Gatekeeper contains a JMX interface for uploading resource mapping files. The interface name is included in the **OAuthResourceMBean**, which can be accessed with the OAM WebLogic interface or using the Services Gatekeeper Platform Test Environment (PTE). You load or retrieve resources using this MBean. See "Using the OAuthResourceMBean" for more information and a list of the supported operations.

Client Management

You can map a client to an existing Services Gatekeeper application instance Id. This mapping lets you use existing SLA enforcement with OAuth security. You manage application clients using the **OAuthClientMBean**, which is available from the OAM WebLogic interface or the Services Gatekeeper Platform Test Environment (PTE). You use this MBean to search for clients or return a list of them. You can also add, remove, or update clients. See "Using the OAuthClientMbean" for more information and a list of the supported operations.

Resource Owner - Resource Mapping

A resource owner for each resource in Services Gatekeeper must be defined to protect the resource. The resource owner is managed using the **OAuthResourceOwnerMBean**. You use this MBean to add, remove, or update resource owners. For all operations, the format of a `resourceScope` is space separated `scopeId` list. See "Creating Resource Owner/Resource Mappings Using Regular Expressions" for more information and a list of the supported operations.

Default Subscriber Manager

Services Gatekeeper acts as an authentication server. You create and authenticate subscribers in the Services Gatekeeper database.

To authenticate users, Services Gatekeeper supports a component called the Subscriber Manager which provisions subscribers, authenticates them, and expands GroupURIs. You manage subscribers using the **SubscriberMBean**. See "Using the SubscriberMBean" for more information and a list of the supported operations.

About Administering OAuth Functionality

Administration of the Services Gatekeeper OAuth server is performed using MBeans in either the WebLogic Administrator console (OAM) or command-line console. For more information about Services Gatekeeper administration, see *Oracle Communications Services Gatekeeper System Administrator's Guide*.

OAuth EAR Files

The OAuth EAR files are deployed as part of the Services Gatekeeper installation.

EDRs and Alarms

The Services Gatekeeper OAuth implementation functions as an application running on the WebLogic application server host. Manual configuration of EDRs and alarms is required if needed. See the chapter on managing and configuring EDRs, CDRs and Alarms in *Oracle Communications Services Gatekeeper Systems Administrator's Guide* for more information.

Deploying and Configuring OAuth Functionality

To deploy and configure the Services Gatekeeper OAuth functionality:

1. Confirm that the OAuth EAR files are deployed.
2. Update OAuth Service configuration using the **OAuthCommonMBean**. See "Using the OAuthCommonMBean" for more information.
3. Create the protected resources in Services Gatekeeper. See "Using the OAuthResourceMBean" for more information.
4. Configure the Authentication URL.
5. Configure the resource owner and define the ownership of resources as described in "Resource Management". Also, see "Creating Resource Owner/Resource Mappings Using Regular Expressions" for more information.
6. Create the client identifier(s) and credentials in Services Gatekeeper that will request access to protected resources. See "Using the OAuthClientMbean" for more information.

See "Example: Protecting the OneAPI Payment Service with OAuth" for an example of the configuration steps.

OAuth Configuration

This section explains how to use the **OAuthCommonMBean** to configure Services Gatekeeper for use with OAuth.

Using the OAuthCommonMBean

Managed object: Container Services, OAuthService

MBean: oracle.Services Gatekeeper.oauth2.management.OAuthCommonMBean

Table 2–1 describes the available attributes.

Table 2–1 Attributes for OAuthCommonMBean

Attributes	Type	Description
TokenType	string	The token type (MAC and Bearer are supported). Default value: **Bearer**
GrantURL	string	The address used to submit a resource owner's grant. Represents the address used to submit a resource owner's grant. The default value is: **https://*host:port*/oauth2/grant** where *host* and *port* are the Services Gatekeeper AT node IP address and HTTPS port.
MacAlgorithm	string	The MAC algorithm used to calculate the request MAC for access token. Default value: **hmac-sha-1**
NoOwnerRequestSupport	boolean	Whether or not no owner is supported. Specifies the OAuth behavior when there is no address (resource owner) information declared in REST API request parameters. **true**: accept such request **false**: reject such request with 401 "invalid_ request" Default value: **true**
GroupUriEnabled	boolean	Whether the group URI option is enabled. Default value: **true**
CleanDbPeriod	int	Number of seconds until the database is cleaned. Default value: **60** seconds
SendAnonymousId	boolean	Whether to include AnonymousId in applyAccessToken response event. Default value: **true**
AuthorizationCodeExpire Period	int	Number of seconds until the authorization code expires. Default value: **600** seconds
IssueRefreshToken	boolean	Whether to issue a refresh token when issuing an access token. Default value: **false**
Authentication URL	string	URL used to authenticate the resource owner and obtain consent for the application requested scope.
IssueRefreshTokenWhenR efresh	boolean	Whether to issue a refresh token when the token is refreshed. Default value: **false**

Table 2–1 (Cont.) Attributes for OAuthCommonMBean

Attributes	Type	Description
TLSUsageForced	boolean	Whether the TLS security protocol is required. For information on setting up and using TLS/SSL security, see *Oracle Fusion Middleware Securing Oracle WebLogic Server 12cRelease*. See the discussion on securing web services in *Oracle Communications Services Gatekeeper Security Guide* for general information on TLS. Default value: **false**

Creating Protected Resources

To enable OAuth protection for RESTful communication services (including custom communication services), communication services can be mapped to OAuth resources.

The resource mapping can then be uploaded to Services Gatekeeper using the **OAuthResourceMBean**.

Using the OAuthResourceMBean

Managed object: Container Services, OAuthService

MBean: oracle.Services Gatekeeper.oauth2.management.OAuthResourceMBean

Following is a list of attributes and operations for the configuration and maintenance of resources.

- Operation: loadResourceXml
- Operation: retrieveResourceXml
- Operation: retrieveResourceList

Operation: loadResourceXml

Scope: Cluster

Loads an XML format resource information file using the **oauth_resource.xsd** schema into Services Gatekeeper.

Signature:

```
loadResourceXml(String xml)
```

See "Resource Mapping" for more information about mapping resources using **oauth_resource.xsd**.

Operation: retrieveResourceXml

Scope: Cluster

Displays resource information in XML format.

Signature:

```
retrieveResourceXml()
```

Operation: retrieveResourceList

Scope: Cluster

Displays resource information in list format.

Signature:

```
retrieveResourceList()
```

Creating Protected Subscription Resources

Services Gatekeeper uses operations in the OAuthResourceMBean to protect subscription resources. For details see the discussion on Services Gatekeeper OAuth 2.0 authorization and resource servers in *Oracle Communications Services Gatekeeper Communication Service Guide*.

Configuring Authentication

In order to grant an authorization code, a resource owner must be authenticated and authorize the scope of the grant. The resource owner can be authenticated using these methods:

- Using the Default Subscriber Manager
- Using Delegated Authentication

A resource owner controls its resources and can allow a client to access them. For each resource, one or more resource owners need to be defined using the SubscriberMBean.

Using the Default Subscriber Manager

Services Gatekeeper offers a built-in subscriber repository to authenticate subscribers. To use the default Subscriber Manager to authenticate subscribers, do the following:

1. Create the subscribers in Services Gatekeeper using the **SubscriberMBean**. This MBean can be accessed through the OAM Console or the PTE Tools MBean browser. See "Using the SubscriberMBean" for more information.
2. Verify that the `AuthenticationURL` property of **OAuthCommonMbean** is set to:

   `https://`*`app_server_IP:app_server_port`*`/oauth2/auth.jsp`

Using the SubscriberMBean

Managed object: Container Services, SubscriberService

MBean: oracle.Services Gatekeeper.subscriber.management.SubscriberMBean

This MBean supports these operations to configure and maintain subscribers:

- Operation: addSubscriber
- Operation: getSubscriberInfo
- Operation: removeSubscriber
- Operation: updateSubscriber
- Operation: verifySubscriber

Operation: addSubscriber

Scope: Cluster

Adds a new subscriber to the Services Gatekeeper authentication server.

Signature:

```
addSubscriber ()
```

Table 2–2 describes the attributes used to create a subscriber in Services Gatekeeper.

Table 2–2 Attributes for New Subscriber

Attributes	Type	Description
Address	string	Subscriber address
LoginId	string	Subscriber login ID
password	string	Subscriber password

Operation: getSubscriberInfo

Scope: Cluster

Retrieves subscriber information using an address or login ID.

Signature:

```
getSubscriberInfo()
```

Table 2–3 describes the attributes used to query a subscriber's info in Services Gatekeeper.

Table 2–3 Attributes for Querying Subscriber Info

Attributes	Type	Description
Address	string	Subscriber address
LoginId	string	Subscriber login ID

Operation: removeSubscriber

Scope: Cluster

Removes a subscriber by address.

Signature:

```
removeSubscriber()
```

Table 2–4 describes the attributes used to remove a subscriber in Services Gatekeeper.

Table 2–4 Attributes for Removing a Subscriber

Attributes	Type	Description
Address	string	Subscriber address

Operation: updateSubscriber

Scope: Cluster

Updates a subscriber's properties.

Signature:

```
updateSubscriber()
```

Table 2–5 describes the attributes used to update a subscriber in Services Gatekeeper.

Table 2–5 Attributes for Updating a Subscriber

Attributes	Type	Description
Address	string	Subscriber address
LoginId	string	Subscriber login ID

Table 2–5 (Cont.) Attributes for Updating a Subscriber

Attributes	Type	Description
password	string	Subscriber password

Operation: verifySubscriber

Scope: Cluster

Verifies a subscriber's address and password.

Signature:

```
verifySubscriber()
```

Table 2–6 describes the attributes used to verify a subscriber in Services Gatekeeper.

Table 2–6 Attributes for Verifying a Subscriber

Attributes	Type	Description
Address	string	Subscriber address
password	string	Subscriber password

Using Delegated Authentication

Instead of provisioning users in the Services Gatekeeper database, you can delegate authentication to a custom authentication server.

See "Implementing a Third-Party Authentication Service" for more information

See "Understanding the OAuth Resource Format" for details on the resource format.

Creating the Resource Owner/Resource Mapping

Protecting resources requires assigning them to owners using the **OAuthResourceOwnerMBean**. This MBean can be accessed either through the OAM Console or using the PTE Tools MBean browser.

The following sections describe how to create owner/resource mappings.

- Creating Resource Owner/Resource Mappings Using Regular Expressions
- Creating Individual Resource Owner/Resource Mappings

See "Understanding the OAuth Resource Format" for details of the resource format.

Creating Resource Owner/Resource Mappings Using Regular Expressions

Managed object: Container Services, OAuthService

MBean: oracle.Services Gatekeeper.oauth2.management.OAuthResourceOwnerMBean

Create an XML rules file that defines the resource owner/resource mapping and upload it to Services Gatekeeper using the OAuthResourceMBean's `loadResourceRuleXml` operation. See `resource_rule.xsd` for the schema definition.

This rules file maps resource owner addresses, represented by a regular expression, to a list of one or more resources. The rules file is interpreted when OAuth grants the authorization, and rules must be defined in order of priority from most specific to most general.

In the following example, owner/resource mapping rules are defined with the most specific rules at the beginning of the file, proceeding to the most general rules at the

end. Placing a more specific rule, with a regular expression such as `^1390.*$`, at the start of the file ensures that the expected cases are caught and correctly interpreted first. Then the rules with more general regular expressions, such as `^.*$`, toward the end of the file serves as a stop gaps to catch the unexpected or rarer cases.

Example 2–1 Regular Expression Rules File

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:addressResourceRules
xmlns:tns="http://oracle/ocsg/oauth2/management/resource_rule"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<!-- numbers start with '1390' own the 'location' and 'payment' services  -->
<tns:rule addressPattern="^1390.*$" resources="location payment"/>
<!-- numbers start with '139' own the 'location' service  -->
<tns:rule addressPattern="^139.*$" resources="location"/>
<!-- All other resources are protected and no resource owners are defined. -->
<!-- Any request with a scope not defined in this xml file will be rejected. -->
<tns:rule addressPattern="^.*$" resources=""/>
</tns:addressResourceRules>
```

These operations configure a resource using regular expressions.

- Operation: loadResourceRuleXML
- Operation: retrieveResourceRuleXML

Operation: loadResourceRuleXML

Scope: Cluster

Loads resource rules defined in an XML file. See Example 2–1, "Regular Expression Rules File" for an example XML file.

Signature:

```
loadResourceRuleXml(String fileContent)
```

Table 2–7 describes these parameters.

Table 2–7 Parameters for loadResourceRuleXML

Parameter	Description
fileContent	An XML file containing rule definitions.

Operation: retrieveResourceRuleXML

Scope: Cluster

Retrieves the current rules XML file.

Signature:

```
updateResourceOwner(String address, String resourceScope)
```

Table 2–8 describes these parameters.

Table 2–8 Parameters for retrieveResourceRuleXML

Parameter	Description
address	Address of the resource owner. The format of address depends on which resource the client trying to access. For most communication services, only **tel:**[+][**0-9**]+ is supported, for example: `tel:15415550100` For SIP-related services, the SIP URI is supported.
resourceScope	The value of an id attribute (`scopeId`) which is defined as part of a resource. This `scopeId` is submitted as part of the authorization grant request. The resource owner grants authorization for the scope (API, method, parameters) defined by this `scopeId`.

Creating Individual Resource Owner/Resource Mappings

Managed object: Container Services, OAuthService

MBean: oracle.Services Gatekeeper.oauth2.management.OAuthResourceOwnerMBean

These operations configure individual resource owners.

- Operation: addResourceOwner
- Operation: updateResourceOwner
- Operation: removeResourceOwner
- Operation: getResourceOwnerInfo

Operation: addResourceOwner

Scope: Cluster

Adds a resource owner in Services Gatekeeper.

The value of the id attribute, `scopeId`, creates a resource owner for a resource. This `scopeId` is the value of the `resourceScope` parameter.

Signature:

```
addResourceOwner(String address, String resourceScope)
```

Table 2–9 describes these parameters.

Table 2–9 Parameters for addResourceOwner

Parameter	Description
address	Address of the resource owner. The format of address depends on which resource the client trying to access. For most communication services, only **tel:**[+][**0-9**]+ is supported. For example: `tel:15415550100` For SIP-related services, the SIP URI is supported.
resourceScope	The value of an id attribute (`scopeId`) which is defined as part of resource. This `scopeId` is submitted as part of the authorization grant request. The resource owner grants authorization for the scope (API, method, parameters) defined by this `scopeId`.

Operation: updateResourceOwner

Scope: Cluster

Updates the properties of a resource owner.

Signature:

```
updateResourceOwner(String address, String resourceScope)
```

Table 2–10 describes these parameters.

Table 2–10 Parameters for updateResourceOwner

Parameter	Description
address	Address of the resource owner
resourceScope	Scope of the resource identified by scopeId.

Operation: removeResourceOwner

Scope: Cluster

Removes a resource owner (by address).

Signature:

```
removeResourceOwner(String address)
```

Table 2–11 describes these parameters.

Table 2–11 Parameters for removeResourceOwner

Parameter	Description
address	Address of the resource owner

Operation: getResourceOwnerInfo

Scope: Cluster

Retrieves resource owner information (by address).

Signature:

```
getResourceOwnerInfo(String address)
```

Table 2–12 describes these parameters.

Table 2–12 Parameters for getResourceOwnerInfo

Parameter	Description
address	Address of the resource owner

Configuring Clients

Services Gatekeeper allows the creation of an application client to support the authorization code grant type. A client registers with its password and the allowed redirect URI in Services Gatekeeper. The **OAuthClientMBean** configures application clients, and can be accessed either through the OAM Console or using the PTE Tools MBean browser. See "Using the OAuthClientMbean" for more information.

Using the OAuthClientMbean

Managed object: Container Services, OAuthService

MBean: oracle.Services Gatekeeper.oauth2.management.OAuthClientMBean

These attributes and operations configure and maintain clients.

- Operation: addClient
- Operation: removeClient
- Operation: getClientInfo
- Operation: listClients
- Operation: searchClients
- Operation: updateClient

Operation: addClient

Scope: Cluster

Adds an application client to Services Gatekeeper.

Signature:

```
addClient(String id, String name, String password, String description, String
allowedRedirectionURI, Boolean supportImplicitGrant, String appInstanceID)
```

Table 2–13 describes these parameters.

Table 2–13 Parameters for addClient

Parameter	Description
id	Client identifier
name	Client name
password	Client password
description	Client description
allowedRedirectionURI	Allowed redirection URIs, split by a space character (for example, "URI1 URI2 URI3")
supportImplicitGrant	Whether implicit grant is supported
AppInstanceId	Application instance Id in Services Gatekeeper

Operation: removeClient

Scope: Cluster

Removes a client (by Id).

Signature:

```
removeClient(String id)
```

Table 2–14 describes these parameters.

Table 2–14 Parameters for removeClient

Parameter	Description
id	Client identifier

Operation: getClientInfo

Scope: Cluster

Retrieves client information (by Id).

Signature:

```
getClientInfo(String id)
```

Table 2–15 describes these parameters.

Table 2–15 Parameters for getClientInfo

Parameter	Description
id	Client identifier

Operation: listClients

Scope: Cluster

Retrieves a list of all clients.

Signature:

```
listClients(int offset, int size))
```

Table 2–16 describes these parameters.

Table 2–16 Parameters for listClients

Parameter	Description
Offset	Offset within the complete result set. Must be >= 0.
Size	Number of entries to return. 0 means no limit.

Operation: searchClients

Scope: Cluster

Returns a list of clients whose name matches a pattern that you enter.

Signature:

```
List<String> searchClients(String, pattern)
```

Table 2–17 describes these parameters.

Table 2–17 Parameters for updateClient

Parameter	Description
pattern	A regular expression to match client names.

Operation: updateClient

Scope: Cluster

Updates an existing client in Services Gatekeeper.

Signature:

```
updateClient(String id, String name, String password, String description, String
allowedRedirectionURI, Boolean supportImplicitGrant, String appInstanceID)
```

Table 2–18 describes these parameters.

Table 2–18 Parameters for updateClient

Parameter	Description
id	Client identifier
name	Client name
password	Client password
description	Client description
allowedRedirectionURI	Allowed redirection URIs, split by a space character (for example, "URI1 URI2 URI3")
supportImplicitGrant	Whether implicit grant is supported
AppInstanceId	Application instance Id in Services Gatekeeper

Protecting Resources in a New Communication Service

It is possible to create a custom RESTful communication service using the Platform Development Studio (PDS) wizard and deploy the service on the Services Gatekeeper platform. This service is automatically protected by OAuth2.0.

The service must be provisioned as an OAuth2.0 resource as described in the following steps:

1. Deploy the service into the Services Gatekeeper server.

   For example:

   ```
   Interfacename=com.foo.Demo
   Method=bar
   ```

2. Execute the `loadResourceXml` operation in the **OAuthResourceMbean** to create a resource element. For example, use the following XML:

   ```
   <resource id="foo_id " name="Demo Service" interfaceName=" com.foo.Demo"
   methodName=" bar"  tokenExpirePeriod="3600"></resource>
   ```

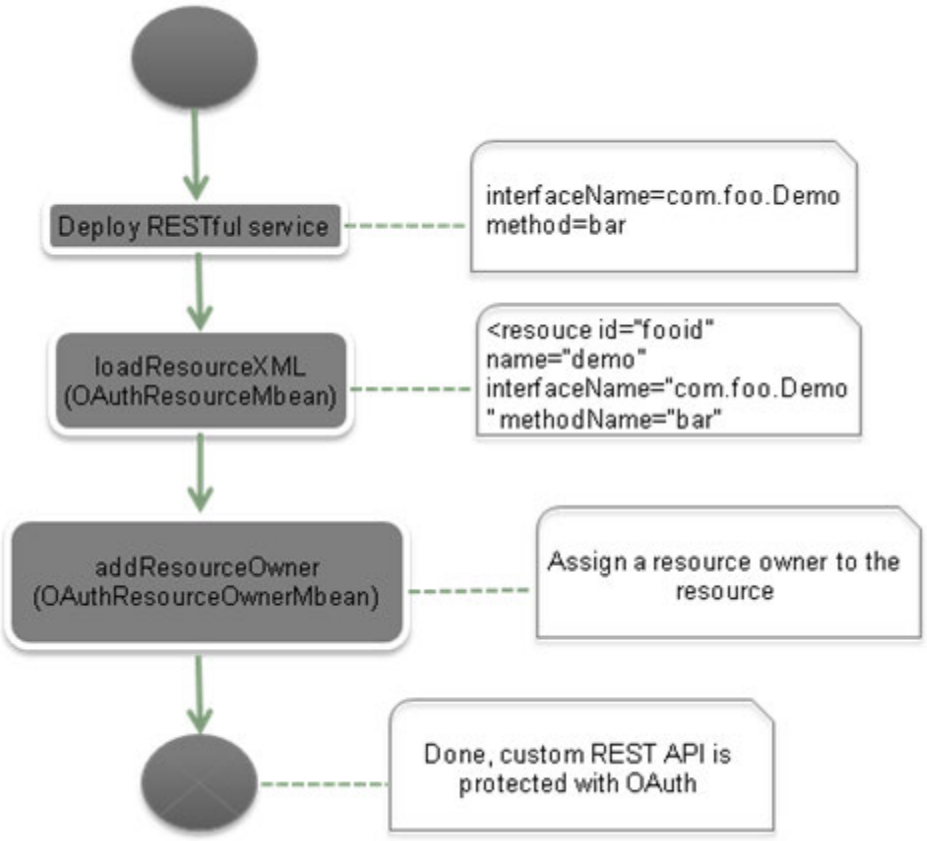
3. Execute the `addResourceOwner` operation in the **OAuthResourceOwnerMbean** with the following values (where the *resource_owner_address* is the TEL:/SIP: URI):

   ```
   address=${resource_owner_address}
   resourceScope=foo_id
   ```

After completing the above steps, the custom RESTful communication service can be accessed if a resource owner grants access to any application client.

Figure 2–1 illustrates the above steps.

Figure 2–1 Protecting a Custom Communication Service



Example: Protecting the OneAPI Payment Service with OAuth

This section explains how to protect the OneAPI Payment Service with OAuth.

Steps to Protecting the OneAPI Payment Service with OAuth

1. Adding a Client in Services Gatekeeper
2. Configuring the Authentication URL
3. Adding One API Payment Communication Service as an OAuth resource
4. Adding a New Subscriber
5. Assigning the Resource to the Subscriber to Act as Resource owner

Adding a Client in Services Gatekeeper

1. Open the MBean browser in PTE or use the OAM to access the **addclient** operation in the **OAuthClient** MBean at:

   Wlng, OauthServer, OauthClientMBean, addClient()

2. Use the following parameters for the `addclient` operation:
   - Id: app123
   - Name: App123_name
   - Password: *password*

- Description: Demo Application
- AllowRedirectURI: `https://localhost/app/redirect.php`
- AppInstanceId: domain_user

3. Submit the parameters to add the new client.

Configuring the Authentication URL

1. Open the MBean browser in PTE or use the OAM to access the AuthenticationURL configuration setting in the OAuthCommon MBean at:

   Wlng, OauthServer, OauthCommonMBean, AuthenticationURL

2. Use the following parameters for the **AuthenticationURL** field:

   - AuthenticationURL: `https://`*app_tier_host*`:`*app_tier_port*`/oauth2/auth.jsp`

3. Submit the parameter to set the authentication URL.

Adding One API Payment Communication Service as an OAuth resource

1. Open the MBean browser in PTE or use the OAM to access the **loadResourceXml** operation in the **OAuthResourceMBean** at:

   Wlng, OauthServer, OauthResourceMBean, loadResourceXml()

2. Use the following sample XML content for the `FileContent` parameter field:

```
<?xml version="1.0" encoding="UTF-8"?>
<resources xmlns="http://oracle/Services Gatekeeper/oauth2/management/xml"
mlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <!--  OneAPI Payment  amountTransaction    -->
  <resource id="POST-/payment/acr:Authorization/transactions/amount"
name="Charge or refund" interfaceName="oracle.Services
Gatekeeper.parlayrest.plugin.PaymentPlugin" methodName="amountTransaction"
tokenExpirePeriod="3600">
  <parameter name="code" description="billable item id"/>
  </resource>
</resources>
```

3. Submit the parameter to add the payment service as an OAuth resource.

Adding a New Subscriber

1. Open the MBean browser in PTE or use the OAM to access the **addSubscriber** operation in the SubscriberMBean at:

   Wlng, SubscriberService, SubscriberMBean, addSubscriber()

2. Use the following parameters for the addSubscriber operation:

   - Address: tel:888
   - LoginID: Jack
   - Password: *password*

3. Submit the parameters to create a subscriber.

Assigning the Resource to the Subscriber to Act as Resource owner

1. Open the MBean browser in PTE or use the OAM to access the **addResourceOwner** operation in the OAuthResourceOwnerMBean at:

   Wlng, OauthServer, OauthResourceOwnerMBean, addResourceOwner()

2. Use the following parameters for the addResourceOwner operation:
   - Address: tel:888
   - resourceScope: `POST-/payment/acr:Authorization/transactions/amount`
3. Submit the parameters to create a subscriber.

Understanding the OAuth Resource Format

The Services Gatekeeper OAuth resource format is defined in the **oauth_resource.xsd** file located in the **oauth2_nt.ear** file. To view the resource schema definition use an archive manager to expand the **wlng_nt_oauth2.ear** found in:

middleware_home`/ocsg_5.1/applications`

Here are the contents of the **oauth_resource.xsd** file:

Example 1 oauth_resource.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<resources xmlns="http://oracle/ocsg/oauth2/management/xml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <!-- OneAPI Payment -->
  <!-- amountTransaction  -->
  <resource id="POST-/payment/tel:15415550100/transactions/amount" name="Charge or
refund"
  interfaceName="oracle.ocsg.parlayrest.plugin.PaymentPlugin"
methodName="amountTransaction"
  tokenExpirePeriod="3600">
  <parameter name="code" description="billable item id"/>
  <subResource>checkTransactionStatus</subResource>
  </resource>

  <!-- list amount transactions -->
  <resource id="GET-/payment/tel:15415550100/transactions/amount" name="list
amount transaction"
    interfaceName="oracle.ocsg.parlayrest.plugin.PaymentPlugin"
methodName="listTransaction"
    tokenExpirePeriod="3600">
  <subResource>checkTransactionStatus</subResource>
  </resource>

  <!-- get amount transaction -->
  <resource id="checkTransactionStatus" name="Get amount transaction detail"
    interfaceName="oracle.ocsg.parlayrest.plugin.PaymentPlugin"
methodName="checkTransactionStatus"
    tokenExpirePeriod="3600"/>

  <!-- start reservation -->
  <resource id="startAmountReservationTransaction"
name="startAmountReservationTransaction"
    interfaceName="oracle.ocsg.parlayrest.plugin.PaymentPlugin"
methodName="startAmountReservationTransaction"
    tokenExpirePeriod="3600"/>

  <!-- update reservation: reserve additional, charge reservation, release
reservation -->
  <resource id="updateAmountReservationTransaction"
name="updateAmountReservationTransaction"
```

```
    interfaceName="oracle.ocsg.parlayrest.plugin.PaymentPlugin"
methodName="updateAmountReservationTransaction"
    tokenExpirePeriod="3600"/>

</resources>
```

Table 2–19 lists the resource structure and attributes.

Table 2–19 Resource Structure and Attributes

Attributes	Type	Description
id	String	Unique identifier for the resource scope (required). As part of an authorization grant, the Id (as the `scopeId`), is submitted as part of the scope-token parameter value.
name	String	Resource name (required). A concise description of a resource which can be used for display purposes.
interfaceName	String	Plug-in north interface name of the resource (required).
methodName	String	Plug-in north method name of the resource (required).
tokenExpirePeriod	Int	Number of seconds until a token expires (optional). If multiple resources (scopes) are granted with a single token, the earliest token expiration period will be enforced on the token. If the resource has subResources, then the earliest token expiration period configured among all resources will be used.
subResource	String	One or more resources that can exist within the scope of the resource (optional). The value of this field should be an id of another resource.
parameter	ResourceParameter	One or more parameters valid for the resource (optional). These parameter(s) are submitted as part of the OAuth authorization grant. During an authorization grant, a resource may accept several parameters, and each of the parameters can have two attributes, name and description. Parameters defined as part of the resource do not need to be directly related to the method parameters of an API. The semantics of the parameters can be interpreted by a custom interceptor by examining the RequestContext. For example, for the following scope value: `chargeAmount?code=123` The chargeAmount is the scopeId mapped in Services Gatekeeper, the code represents the parameter name and 123 represents the parameter value. As part of communication service access (resource access), a custom interceptor can be written to interpret the OAuth token scope and RequestContext and validate the token usage against the authorization scope.

Resource Representation Example

The following is an example XML representation of the OAuth resource mapping for a OneAPI communication service:

```
<?xml version="1.0" encoding="UTF-8"?>
<resources xmlns="http://oracle/Services Gatekeeper/OAuth2.0 /management/xml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <!-- amountTransaction  -->
  <resource id="chargeAmount" name="Charge or refund"
  interfaceName="oracle.Services Gatekeeper.parlayrest.plugin.PaymentPlugin"
```

```
methodName="amountTransaction"
  tokenExpirePeriod="3600">
  <parameter name="code" description="billable item id"/>
  <subResource>checkTransactionStatus</subResource>
  </resource>

  <!-- list amount transactions -->
  <resource id="listAmount" name="List amount transactions"
    interfaceName="oracle.Services Gatekeeper.parlayrest.plugin.PaymentPlugin"
methodName="listTransaction"
    tokenExpirePeriod="3600">
  <subResource>checkTransactionStatus</subResource>
  </resource>

  <!-- get amount transaction -->
  <resource id="checkTransactionStatus" name="Get amount transaction"
    interfaceName="oracle.Services Gatekeeper.parlayrest.plugin.PaymentPlugin"
methodName="checkTransactionStatus"
    tokenExpirePeriod="3600"/>
</resources>
```

The following resources are defined in this example:

- **chargeAmount**: a token can be obtained for this resource, but this restricts the access of the resource (OneAPI charging API) to the code specified as part of the scope parameter value.
- **listAmount**
- **checkTransactionStatus**

In addition, one **subResource** is also defined. The **checkTransactionStatus** subResource is defined as a subResource for the **chargeAmount** and **listAmount** resources. By defining **checkTransactionStatus** as a subResource, Services Gatekeeper facilitates using the same access token obtained for **chargeAmount** while accessing the **checkTransactionStatus** resource.

3

Monitoring OAuth Services in Service Gatekeeper

This chapter explains how to manage an Oracle Communications Services Gatekeeper (Services Gatekeeper) implementation that uses Open Authorization Protocol (OAuth) features.

OAuth Runtime

This section describes the Services Gatekeeper runtime OAuth actions, explains token management, and lists the EDRs and errors that OAuth generates.

Issuing OAuth Tokens

This section explains how Services Gatekeeper manages Oauth tokens.

Default Authentication and Authorization

Services Gatekeeper includes an authorization JSP page to enter resource owner information and validate the scope requested by an application. This page displays the scope and resource details that a resource owner uses to issue an authorization grant to an application.

The `Auth.jsp` that handles the default authentication is located in `oauth2_service.war` at the following location:

middleware_home`/ocsg_5.1/applications/wlng_at_oauth2.ear`

Authorization for Group URIs

The default Subscriber Manager treats a group owner with a group URI as a normal resource owner, so a group owner with a group URI has its own password.

When Services Gatekeeper issues an authorization grant for a given group URI as a resource owner, the token can access a resource on behalf of any of the group members.

The group owner's URI and password authorize an application to access resources that are owned by all member in the group.

You enable or disabled this feature using the **groupUriEnabled** Mbean property in the **OauthCommonMbean**.

See "Securing Resources with Multiple Owners" for more information.

Understanding Token Validation

Services Gatekeeper supplies an interceptor to validate access tokens. The interceptor must be configured with a minimum index value in the interceptor chain to allow validation requests to be handled properly. By default, it is the second interceptor.

The token validation interceptor checks the following:

- Whether the access token is expired.
- Whether the resource owner matches the end user ID in the RESTful API request.
  - An exact match for a resource owner.
  - If token is issued for group URI, then request URI should be a member of the same group.
- Whether requested resource is within the scope of a token.

If the token is a MAC type, additional checks are required for the following:

- Body hash
- Nonce
- Mac

Custom interceptors can be developed and deployed for parameter value checking and token type checking (if MAC Type) of requests.

Token Management

This section describes how to manage OAuth tokens using the JMX interfaces **TokenManagementMBean**, which you access from the OAM WebLogic interface or the Services Gatekeeper Platform Test Environment (PTE). See "Using the TokenMangementMBean" for more information.

Using the TokenMangementMBean

Managed object: Container Services then OAuthService

MBean: `oracle.ocsg.oauth2.management.TokenManagementMBean`

This MBean supports these operations:

- Operation: listAccessTokensByEndUser
- Operation: listRefreshTokensByEndUser
- Operation: listAccessTokensByClientIdAndEndUser
- Operation: listRefreshTokensByClientIdAndEndUser
- Operation: listAccessTokensByClientId
- Operation: listRefreshTokensByClientId
- Operation: countAccessTokensByClientId
- Operation: countRefreshTokensByClientId
- Operation: revokeAccessToken
- Operation: revokeRefreshToken

Operation: listAccessTokensByEndUser

Scope: Cluster

Lists access tokens by the address of an end user.

Signature:

```
listAccessTokensByEndUser(String endUserId)
```

Table 3–1 describes these parameters.

Table 3–1 Parameters for listAccessTokensByEndUser

Parameter	Description
endUserId	resource owner URI.

Operation: listRefreshTokensByEndUser

Scope: Cluster

Lists refresh tokens by the address of an end user.

Signature:

```
listRefreshTokensByEndUser(String endUserId)
```

Table 3–2 describes these parameters.

Table 3–2 Parameters for listRefreshTokensByEndUser

Parameter	Description
endUserID	resource owner URI.

Operation: listAccessTokensByClientIdAndEndUser

Scope: Cluster

Lists access tokens by the client Id in addition to the address of an end user.

Signature:

```
listAccessTokensByClientIdAndEndUser(String clientId, String endUserId)
```

Table 3–3 describes these parameters.

Table 3–3 Parameters for listAccessTokensByClientIdAndEndUser

Parameter	Description
clientID	Client identifier.
endUserId	resource owner URI.

Operation: listRefreshTokensByClientIdAndEndUser

Scope: Cluster

Lists refresh tokens by the client Id in addition to the address of an end user.

Signature:

```
listRefreshTokensByClientIdAndEndUser(String clientId, String endUserId)
```

Table 3–4 describes these parameters.

Table 3–4 Parameters for listRefreshTokensByClientIdAndEndUser

Parameter	Description
clientID	Client identifier.
endUserId	resource owner URI.

Operation: listAccessTokensByClientId

Scope: Cluster

Lists access tokens by the client Id.

Signature:

```
listAccessTokensByClientId(String clientId, int offset, int size)
```

Table 3–5 describes these parameters.

Table 3–5 Parameters for listAccessTokensByClientId

Parameter	Description
clientID	Client identifier.
Offset	Offset within a complete result set. Must be >= 0.
Size	Number of entries to return. 0 means no limit.

Operation: listRefreshTokensByClientId

Scope: Cluster

Lists refresh tokens by the client Id.

Signature:

```
listRefreshTokensByClientId (String clientId, int offset, int size)
```

Table 3–6 describes these parameters.

Table 3–6 Parameters for listRefreshTokensByClientId

Parameter	Description
clientID	Client identifier.
Offset	Offset within a complete result set. Must be >= 0.
Size	Number of entries to return. 0 means no limit.

Operation: countAccessTokensByClientId

Scope: Cluster

Lists the number of access tokens by client Id.

Signature:

```
countAccessTokensByClientId(String clientId)
```

Table 3–7 describes these parameters.

Table 3–7 Parameters for countAccessTokensByClientId

Parameter	Description
clientID	Client identifier.

Operation: countRefreshTokensByClientId

Scope: Cluster

Lists the number of refresh tokens by client Id.

Signature:

```
countRefreshTokensByClientId(String clientId)
```

Table 3–8 describes these parameters.

Table 3–8 Parameters for countRefreshTokensByClientId

Parameter	Description
clientID	Client identifier.

Operation: revokeAccessToken

Scope: Cluster

Revokes an access token.

Signature:

```
revokeAccessToken(String token)
```

Table 3–9 describes these parameters.

Table 3–9 Parameters for revokeAccessToken

Parameter	Description
token	OAuth access token.

Operation: revokeRefreshToken

Scope: Cluster

Revokes a refresh token.

Signature:

```
revokeRefreshToken(String token)
```

Table 3–10 describes these parameters.

Table 3–10 Parameters for revokeRefreshToken

Parameter	Description
token	OAuth access token.

EDRs Generated by the OAuth Service

Table 3–11 describes the EDRs that can be generated by the OAuth service.

Table 3–11 OAuth Service EDRs

EDR ID	Class	Method	Description	Additional Attributes in the EDR
20001	oracle.ocsg.oauth2.interceptor.OAuth2AppListener	postStart	Generated when the OAuth service is started.	None
20002	oracle.ocsg.oauth2.interceptor.OAuth2AppListener	preStop	Generated when the OAuth service is stopped.	None
20003	oracle.ocsg.oauth2.ejb.server.OAuthServiceBean	authorize	Generated when an authorization code is issued to an application.	OAuth2ClientId OAuth2ResourceOwner OAuth2Scopes OAuth2AuthorizeType If the response is a code: OAuth2AuthorizationCode If the response is a token: OAuth2AccessToken OAuth2TokenType
20004	oracle.ocsg.oauth2.ejb.server.OAuthServiceBean	applyToken	Generated when an access token is issued to an application.	OAuth2ClientId OAuth2ResourceOwner OAuth2GrantType OAuth2AuthorizationCode OAuth2AccessToken OAuth2TokenType If a refresh token is generated: OAuth2RefreshToken
20005	oracle.ocsg.oauth2.ejb.server.OAuthServiceBean	refreshToken	Generated when an application requests a refresh token.	OAuth2ClientId OAuth2ResourceOwner OAuth2GrantType OAuth2OrignalRefreshToken OAuth2AccessToken OAuth2TokenType If a refresh token is generated: OAuth2RefreshToken
20006	oracle.ocsg.oauth2.interceptor.OAuth2Interceptor	invoke	Generated when an application accesses a resource with an OAuth access token.	OAuth2ClientId OAuth2ResourceOwner OAuth2AccessToken OAuth2TokenType OAuth2ResourceClass OAuth2ResourceMethod

OAuth/Services Gatekeeper Errors and Exceptions

Table 3–12 describes the error conditions and resulting operation responses provided by the Services Gatekeeper OAuth 2.0 authorization server.

Table 3–12 Exception Scenarios

Type	Error	Response

invalid_ request	The request is missing a required parameter, includes an invalid parameter value, or is otherwise malformed.	`HTTP/1.1 400 Bad Request`
		`Content-Type: application/json`
		`Cache-Control: no-store`
		`{`
		`"error":"invalid_request"`
		`}`

invalid_realm	No authentication header with the default Services Gatekeeper realm	`HTTP/1.1 401 Unauthorized` `WWW-Authenticate: realm="default"`

invalid_grant	The provided authorization grant (for example authorization code or resource owner credentials) is invalid, expired, revoked, and does not match the redirection URI used in the authorization request, or was issued to another client.	`HTTP/1.1 400 Bad Request`
		`Content-Type: application/json`
		`Cache-Control: no-store`
		`{`
		`"error":"invalid_grant"_`
		`}`

invalid_client	Client authentication failed (for example, unknown client, no client authentication included, or unsupported authentication method). The authorization server may return an HTTP 401 (Unauthorized) status code to indicate which HTTP authentication schemes are supported. If the client attempted to authenticate using the authorization request header field, the authorization server must respond with an HTTP 401 (Unauthorized) status code, and include the WWW-Authenticate response header field matching the authentication scheme used by the client.	`HTTP/1.1 400 Bad Request`
		`Content-Type: application/json`
		`Cache-Control: no-store`
		`{`
		`"error":"invalid_client"_`
		`}`

Table 3–12 (Cont.) Exception Scenarios

Type	Error	Response
unauthorized _client	The client is not authorized to request an authorization code using this method.	`HTTP/1.1 401 Unauthorized`
unauthorized _owner	Invalid resource owner credential in the authorization request	`HTTP/1.1 401 Unauthorized`
insufficient_ scope	Insufficient scope in the authorization request	`HTTP/1.1 403 Forbidden`
invalid_token	Invalid resource owner's credential the authorization request	`HTTP/1.1 401 Unauthorized`
invalid_token	Duplicated authorization code in the authorize request	`HTTP/1.1 401 Unauthorized`
insufficient_ scope	Invalid scope in the refresh token request	`HTTP/1.1 403 Forbidden`
invalid_token	Discarded refresh token in the refresh token request	`HTTP/1.1 401 Unauthorized`

invalid_token	No authenticate header When using MAC-type access token to access resource	`HTTP/1.1 401 Unauthorized`
		`WWW-Authenticate: MAC`
		` error="invalid_token",`

invalid_token	Invalid MAC-type access token When accessing resource	`HTTP/1.1 401 Unauthorized` `WWW-Authenticate: MAC`

invalid_token	No Authenticate header When using Bearer-type access token to access resource	`HTTP/1.1 401 Unauthorized`
		`WWW-Authenticate:`
		` error="invalid_token",`

invalid_token	Invalid Bearer-type access token when accessing resource	`HTTP/1.1 401 Unauthorized`
		`WWW-Authenticate:`
		` error="invalid_token",`

insufficient_ scope	The request requires higher privileges (scope) than provided by the access token	`HTTP/1.1 403 Forbidden`

access denied	The resource owner or authorization server denied the request.	`HTTP/1.1 302 Found`
		`Location:`
		`https://client.example.com/cb?error=access_`
		`denied&state=xyz`

unsupported _response_ type	The authorization server does not support obtaining an authorization code using this method.	`HTTP/1.1 302 Found`
		`Location:`
		`https://client.example.com/cb?error=unsuppor`
		`ted_response_type`

Table 3–12 (Cont.) Exception Scenarios

Type	Error	Response

unsupported _grant_type	The authorization grant type is not supported by the authorization server.	`HTTP/1.1 400`
		`Location:`
		`https://client.example.com/cb?error=unsupported_grant_type`

invalid_scope	The requested scope is invalid, unknown, or malformed.	`HTTP/1.1 302 Found`
		`Location:`
		`https://client.example.com/cb?error=invalid_scope`

server_error	The authorization server encountered an unexpected condition which prevented it from fulfilling the request.	`HTTP/1.1 400`
		`error="server_error",`
		
		The HTTP response code for `server_error` depends on which endpoint is responding.
		The Authorization and Grant endpoints return 302 error responses as defined by the OAuth specification.
		The Services Gatekeeper Token endpoint returns a 400 error response.

temporarily_ unavailable	The authorization server is currently unable to handle the request due to a temporary overloading or maintenance of the server.	Not Supported

other	Undetermined	`HTTP/1.1 500`
		`Content-Type: application/json`
		`Cache-Control: no-store`
		
		`{`
		`"error":"500"`
		`}`

4

Developing Services Gatekeeper Services Using OAuth

This chapter explains the options you have for customizing the Open Authorization Protocol (OAuth) functionality for use with Oracle Communications Services Gatekeeper (Services Gatekeeper).

Customization

This section contains information on customizing Service Gatekeeper's OAuth functionality.

Implementing a Third-Party Authentication Service

You can delegate authentication to a third-party authentication service provider instead of with the default Subscriber Management Service. The authentication provider is responsible for the resource owner identity validation and handling the grant collection flow.

A delegated authentication service used with Services Gatekeeper is responsible for:

1. Hosting the Authentication Endpoint.
2. Presenting the expanded scope and authenticating a resource owner.
3. Redirecting the resource owner to the grant endpoint hosted by Services Gatekeeper upon successful authentication of the resource owner.

See "Understanding the OAuth Endpoints" for more information.

Authentication Process Flow

This section describes the flow of requests between Services Gatekeeper and a delegated authentication service. Sample responses to the requests along with a description of the flow are provided.

1. An application sends a standard OAuth2.0 Authorization request to Services Gatekeeper in a format that looks like this:

   ```
   GET /oauth2/authorize?client_id=client123&redirect_
   uri=https://www.google.com/asdf&response_
   type=code&scope=POST-/payment/acr:Authorization/transactions/amount&state=123
   HTTP/1.1
   ```

   After receiving the OAuth2 authorization request, Services Gatekeeper add more detailed information to it using the **client_id** and **scope** request parameters. This

additional information is appended to the location header in the 302 redirect response directed to the configured authentication endpoint.

The location header contains these elements:

- The delegating authentication endpoint
- The original OAuth2.0 Authentication request parameters
- The Grant endpoint
- Detailed information for the **client_id** and scope parameters.

An example 302 response is provided here:

```
HTTP/1.1 302 Moved Temporarily
Location: https://authentication_url?client_id=client123&redirect_
uri=https://www.google.com/asdf&response_
type=code&scope=POST-/payment/acr:Authorization/transactions/amount&state=123&g
rant_url=grant&client_
info=%7B%22clientId%22%3A%22client123%22%2C%22clientName%22%3A%22client123%22%2
C%22clientDescription%22%3A%22client123+desc%22%7D&scopes_
info=%5B%7B%22scopeId%22%3A%22POST-%2Fpayment%2Facr%3AAuthorization%2Ftransacti
ons%2Famount%22%2C%22scopeDescription%22%3A%22Charge+or+refund%22%2C%22paramete
rs%22%3A%5B%7B%22code%22%3A%22billable+item+id%22%7D%5D%7D%5D
```

In addition to the original OAuth2.0 authorization request parameters, the detailed format specs of all additional parameters are defined in Table 4–1:

Table 4–1 OAuth 2.0 Authorization Request Parameters

Parameter	Description
grant_url	The URL can be submitted later according resource owner's approval. See "Understanding the OAuth Endpoints" for more information.

client_info	Client information will be constructed into a JSON Object as shown below. Encoding complies with the following specification: http://www.w3.org/Addressing/URL/url-spec.html
	{
	"clientId":"client123",
	"clientName":"Oracle",
	"clientDescription":"Oracle Description"
	}

scopes_info	scope information will be constructed into a JSON Object as shown below. Encoding complies with the following specification: http://www.w3.org/Addressing/URL/url-spec.html
	[
	{
	"scopeId":"POST- payment acr:Authorization transactions amount",
	"scopeDescription":"Charge+or+refund",
	"parameters":[{"code":"billable+item+id"}]
	}
	]

2. The resource owner's browser continues to access the authentication endpoint identified in the Location Header.

The Authentication endpoint should accept the redirected request, authenticate the resource owner for proper credentials and render an interactive graphical interface for authorization. The resource owner can use the information in the interface to understand the scope and client information of the authorization request and determine if the request should be authorized.

After the resource owner authorizes the scope the Authentication endpoint redirects the resource owner to the Grant endpoint with following parameters through an HTTP POST operation. The OAuth flow continues normally after redirecting the resource owner toward the grant endpoint. The client then receives the authorization code at the Redirect endpoint.

Table 4–2 lists the OAuth 2.0 grant endpoint POST parameters.

Table 4–2 OAuth 2.0 Grant Endpoint POST Parameters

Parameter	Description
user_address	Address of resource owner
grant_scopes	The scope that the resource owner grants to the application. The value of the scope parameter is expressed as a list of space-delimited strings. Each string adds an additional access range to the selected scope parameter. According to the resource owner decisions at the Authentication endpoint, the granted scope can be narrower than the originally requested scope. Services Gatekeeper will reject a granted scope that is wider than originally requested scope. Based on the implementation of the Authentication endpoint and the resource owner interaction, additional parameter may be appended to each scope id. These scope parameters will be available to an interceptor so that stricter enforcement can be applied according to different parameters. The scope format is: scopeId?[<*param*>=<*value*>[&<*param*>=<*value*>]*]. For example: `grant_scopes=chargeAmount?maxAmount=100&minAmount=100 getLocation?requestedAccuracy=100 sendSMS`
response_type	As in the first authorization request
client_id	As in the first authorization request
redirect_uri	As in the first authorization request
state	As in the first authorization request
scope	As in the first authorization request

Creating an OAuth Interceptor

This section describes the basic principles for creating a custom OAuth interceptor.

As described in "Implementing a Third-Party Authentication Service", it is possible to add additional parameters to the scope-token so that custom interceptors can be created for fine-grained resource access and traffic control.

Table 4–3 lists the OAuth parameters available in the `RequestContext` object for an OAuth2.0 enabled communication service. Customized interceptors can make use of these parameters to further fine tune authorized access to protected resources.

For information on creating custom interceptors, see *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*.

Table 4–3 OAuth 2.0 RequestContext Parameters

Attribute Name	Access	Type	Description
OAUTH2_SCOPE_PARAMETER	read only	java.util.Map	Contains all parameters of the current request scope.
CONTEXT_OAUTH2_RESOURCE_ OWNER	read only	java.lang.String	The resource owner of the token, which is usually the same as the address in the request. When the resource owner is a group URI or the scheme of address in request is ACR, they may be different.
CONTEXT_OAUTH2_PARAMETER	read only	java.util.Map	Contains all endpoint parameters of this request. This parameter must start with "oracle_" or "ocsg_".
CONTEXT_OAUTH2_STATE	read/write	java.util.Map	Values of this attribute will be available during the lifecycle of one OAuth access token.

Examples: Using a Custom OAuth Interceptor to Retrieve OAuth Information

Below is an example for retrieving and using OAuth associated information from the `requestContext` within a customized interceptor.

To retrieve the MSIDN of an OAuth resource owner:

```
/**
* The following example shows a way to retrieve Oauth2 resource owner MSIDN
*/
@Override
public Object invoke(final Context context) throws Exception {
  String currentResourceOwner = (String) context.getRequestContext().get("CONTEXT_
OAUTH2_RESOURCE_OWNER");
  If (currentResourceOwner == null)
throw new DenyPluginException("Not a OAuth based request!");
  else
System.out.println("Current Oauth2 resource owner is:" + currentResourceOwner);
  context.invokeNext(this);
}
```

To control the maximum charged value using an additional scope parameter called maxAmount:

```
/**
* The following example shows a way to control the maximum charged value using
additional scope parameter
* "maxAmount".
*/
@Override
public Object invoke(final Context context) throws Exception {
if (context.getType().equals(AmountCharingPlugin.class)) {
    Map<String, String> scopeParameters = (Map<String,
String>)context.getRequestContext().get("OAUTH2_SCOPE_PARAMETER");
int maxAmount = Integer.parseInt(scopeParameters.get("maxAmount").toString());

if (((ChargeAmount)context.getArguments()[0]).getAmount() > maxAmount)
  throw new DenyPluginException("Specified chargeAmount request exceed
limitation.");
 }
  context.invokeNext(this);
}
```

Integrating a Third-Party Subscriber Repository

Service Gatekeeper offers the flexibility to integrate with custom subscriber repositories for user authentication. You can develop a customized Subscriber Manager to authenticate users against external subscriber repositories such as LDAP.

Developing a custom Subscriber Manager involves the following steps:

1. Implementing `oracle.Services Gatekeeper.subscriber.SubscriberManager`, and customizing the implementation of this interface
2. Registering the custom implementation with the OAuth security framework with this method.

   ```
   void oracle.Services
   Gatekeeper.subscriber.SubscriberManager.registerInstance("default",
   SubscriberManager instance);
   ```

   For additional information on customizing the default Subscriber Manager, including method details, see the Services Gatekeeper JavaDoc.

Creating an OAuth2.0 Extension Handler

Services Gatekeeper supports a rich set of credential types that OAuth uses for security. However, if your implementation uses new or evolving credential standards that Services Gatekeeper does not support, you have the option to create a customized extension handler to use them. The Platform Development Studio enables you to customize endpoint parameters, grant types, response types, or errors using the **OAuth2 Extension Handlers** wizard.

For details see *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*

Customizing OAuth Resource Grant Tests

Services Gatekeeper enables you to add your own customized tests to OAuth resource requests. For example, you may want to restrict access to a resource to just subscribers from a specific block of email addresses. There are two ways to add the customized tests:

- Using an `auth.jsp` file which you then reference using a `REGEX_MATCH` parameter in the resource XML file. Services Gatekeeper then perform any tests (regular expressions) that you have added to the `jsp` file. Each subscriber must pass the tests in this file to get access to the resource.
- Creating a custom services interceptor.

For details on both of these methods, see *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*.

Application Developer Guide

This section contains information helpful to Application Developers using OAuth2.0 with Services Gatekeeper.

Interacting with the Services Gatekeeper OAuth Service

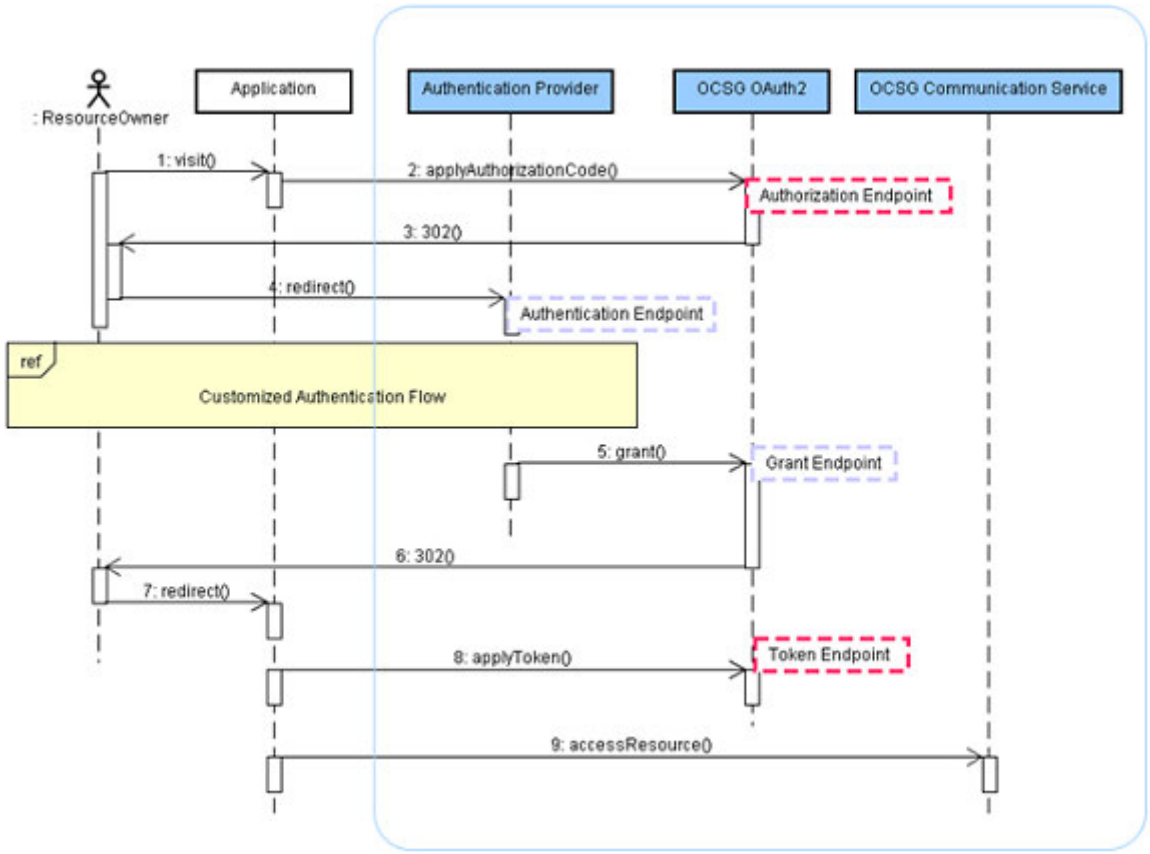
This section describes what OAuth endpoints are available, what steps are involved in obtaining an access token and how an application can use an access token to access a REST resource in Services Gatekeeper.

The following endpoints are available in the OAuth2.0 Service:

- Authorization endpoint
- Token endpoint
- Authentication endpoint
- Grant endpoint

Figure 4–1 demonstrates the end to end flow to obtain an access token and use the access token to access the resource.

Figure 4–1 OAuth Endpoints and Functional Responsibility



OAuth Access Flow In Services Gatekeeper

The following procedure describes the OAuth access flow:

1. A resource owner visits an application Web site and initiates a request that requires granting access to protected resources to an application.
2. The application redirects the resource owner to the **Authorization Endpoint** with the application information including the client id and scope id.

   For example, the application can provide a link to trigger a HTTP GET request where the following information is included in the HTTP query string:

   - **HTTP Request:** `GET`

- **URI**: `https://host:port/oauth2/authorize`
- **Parameters**:
  - **response_type** -- Supported values are code or token
  - **client_id**. -- The client identifier
  - **redirect_uri** -- Required
  - **scope** -- The scope of the access request expressed as a list of space-delimited, case sensitive strings. The Services Gatekeeper Authorization Server accepts zero to multiple scope-tokens in the following format for scope-token:

    <scopeId>[?<*param*>=<*value*>[&<*param*>=<*value*>]*]+

    where **scopeId** is the resource identifier and **param** is the name of one of the allowed parameters defined as part of resource.

    For example:

    chargeAmount?code=1976

    An example scope would look like:

    ```
    GET /oauth2/authorize?response_type=code&client_id=app123&state=xyz
    &redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1

    Host: server.Services Gatekeeper.com
    ```

3. Services Gatekeeper validates the resource owner identity and obtains the resource owner's consent on the requested scope.
4. The application exchanges the authorization code for an authorization token using the Token Endpoint. Services Gatekeeper server returns the token directly.

   The request can be described as follows:

   - **HTTP Request**: `POST`
   - **URI**: `https://<AT_HOST>:<AT_PORT>/oauth2/token`
   - **Parameters**:
     - **grant_type**: Value can be set to authorization_code, if the request is not a SAML assertion.
     - **code**: The authorization code received from the Authorization Server.
     - **redirect_uri**: The redirection URI used by the Authorization Server to return the authorization response in the previous step.
     - **client_id**: The client identifier.
     - **client_secret**: The client password.
   - **Authorization Header**:

     The client application may use the http Basic authentication scheme as defined in RFC2617 to authenticate with the Services Gatekeeper server. The `client_id` is used as the username and the `client_secret` is used as the password.

     For example:

     ```
     Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
     ```

     Alternatively, the Authorization Server may support including the client credentials in the request body using the following parameters:

  - **client_id**: The client identifier.
  - **client_secret**: The application password.

- **HTTP Response:**
  - **access_token**: The authorization code generated by Services Gatekeeper.
  - **token_type**: The Bearer or MAC authorization code received from Services Gatekeeper.
  - **expires_in**: The duration in seconds of the access token lifetime.
  - **refresh_token**: The refresh token which you use to obtain new access tokens using the same authorization grant.
  - **scope**: The scope of the access request expressed as a list of space-delimited, case sensitive strings.
  - **anonymous_id**: Uniquely identifies the resource owner.
  - **mac_key**: The MAC key verifies the later request of access protect resource. (MAC-Type access token).
  - **mac_algorithm**: The MAC algorithm used to calculate the request MAC. The value must be either hmac-sha-1 or hmac-sha-256.

  The response will be different depending on the token type submitted in the request.

  This is an example for a Bearer-Type Access Token with HTTP Basic Authentication:

  Request:

```
POST /oauth2/token HTTP/1.1
Host: localhost:7999
Content-length: 128
Authorization: Basic YXBwMTIzOmFwcDEyMw==
Content-Type: application/x-www-form-urlencoded
Connection: Close

grant_type=authorization_
code&code=75dfe1c9-9784-4545-846f-e1493f087017&redirect_
uri=http%3A%2F%2Flocalhost%2Fapp%2Fredirect.php
```

  Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store
Connection: close
Content-Length: 327
Content-Type: application/json

{"access_token":"44fb85f8-e400-41b3-9bd4-68617d131039","token_
type":"MAC","expires_
in":3600,"scope":"POST-/payment/acr:Authorization/transactions/amount","mac
_algorithm":"hmac-sha-1","mac_
key":"-36776566982993274 87","secret":"-36776566982993274 87","anonymous_
id":"1debde44-f9d4-41d6-88fe-bbb77fea37c8","algorithm":"hmac-sha-1"}
```

  The following example is for a MAC-Type Access Token with included client credentials in the request body.

  Request:

```
POST /oauth2/token HTTP/1.1
Host: server.Services Gatekeeper.com
Content-Type: application/x-www-form-urlencoded
   grant_type=authorization_code&client_id=app123&client_
secret=app123&code=i1WsRn1uB1&redirect_
uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store

{  "access_token":"SlAV32hkKG",    "token_type":"mac",    "expires_
in":3600,    "refresh_token":"8xLOxBtZp8",    "secret":"23sasd#adf@#"
"algorithm":"hmac-sha-1"}
```

5. The application now access the protected resource.

   The application needs to add an HTTP Authorization Header when accessing the granted resource. The value of authorization head depends on the access token type.

   For a Bearer token, the application can directly transmit the access token using an HTTP authorization header in the request.

   For a MAC token, the application constructs the HTTP authorization header using a MAC key with the access token. For more information, see: http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-00.

   Below is a sample PHP code snippet illustrating the insertion of the token in the HTTP Authorization Header:

```
$body_hash=base64_encode(hash('sha1',$http_body,true));
$payload=$nonce."\n".$http_method."\n".$request_path."\n".$host_
name."\n".$host_port."\n".$body_hash."\n".$ext."\n";
$mac = base64_encode(hash_hmac('sha1', $payload, $mac_key, true));
$oauth2_header='MAC id="'.$mac_key_
id."\",nonce=\"".$nonce."\",bodyhash=\"".$body_hash."\",mac=\"".$mac.'"';
```

   Following is an example of a request containing a Bearer authorization token:

```
POST /oneapi/1/payment/acr%3AAuthorization/transactions/amount HTTP/1.1
     Host: localhost:7999
     Content-Type: application/x-www-form-urlencoded
     Authorization: Bearer vF9dft4qmT

{"amountTransaction":{"endUserId":"acr:Authorization",
"paymentAmount":{"chargingInformation":{"description":"chargeAmount",
"currency":"USD",
"amount":"2","code":""},
"chargingMetaData":{"onBehalfOf":"Example Games Inc",
"purchaseCategoryCode":"Game",
"channel":"",
"taxAmount":"0",
"mandateId":"",
"serviceId":"",
"productId":""}},
"transactionOperationStatus":"Charged",
"referenceCode":"REF-12345",
"clientCorrelator":""}
}
```

Following is an example of a request containing a MAC authorization token:

```
POST /oneapi/1/payment/acr%3AAuthorization/transactions/amount HTTP/1.1
Host: localhost:7999
Content-length: 415
Authorization: MAC id="176c04f0-d4d4-4385-b2d6-b19649f21b78",
nonce="273156:di3hvdf8",
bodyhash="junEVZu4M9q1qVaxAByY7lYQun8=",
mac="TudmT3bM5UgqvkL8nq1EuhcZ6O8="
Content-Type: application/json
X-Session-ID: app:-7562122823730178188
Connection: Close

{"amountTransaction":{"endUserId":"acr:Authorization",
"paymentAmount":{"chargingInformation":{"description":"chargeAmount",
"currency":"USD",
"amount":"2",
"code":""},
"chargingMetaData":{"onBehalfOf":"Example Games Inc",
"purchaseCategoryCode":"Game",
"channel":"",
"taxAmount":"0",
"mandateId":"",
"serviceId":"",
"productId":""}},
"transactionOperationStatus":"Charged",
"referenceCode":"REF-"
}
```