ORACLE CLOUD SHARED IDENTITY MANAGEMENT

(**Oracle Internal Document – Do NOT Distribute Outside Oracle**)

Scope and Purpose

This document provides a high-level description of Oracle Shared Identity Management (SIM). This document includes introductory information intended for Oracle Cloud developers, administrators, and DevOps. The appendix at the end of the document includes a Security Assertions Markup Language (SAML) and Open Authorization (OAuth) primer strictly limited to the SIM context.

Abbreviations and Acronyms

The following table lists the acronyms and abbreviations most commonly used in the context of Oracle Cloud's Shared Identity Management (in alphabetical order).

Acronym	Definition	Description
AD	Microsoft Active Directory	Microsoft's LDAP directory for Windows domain networks, used to manage user information for access control purposes.
ADFS	Microsoft AD Federation Services	Microsoft's identity federation system supporting SAML and other industry standards. ADFS uses AD to manage user information.
CRUDQ	Create, Read, Update, Delete, Query	Typical set of operations carried out on data, e.g., user information in a directory or database.
FA	Oracle Fusion Applications	Oracle's cloud-based business applications.
IaaS	Infrastructure as a Service	Oracle's elastic compute and storage services leveraging Oracle's engineered systems.
IDCS	Identity Cloud Service	Future OPC security system offered as a service (SIM's successor). IDCS was formerly known as IDaaS (Identity as a Service).
IdP	Identity Provider	In a business partnership, the asserting party responsible for generating standard identity tokens.
JIT	Just-In-Time Provisioning	The ability for a SAML-based federation service in SP mode to provide the tenant administrator with a feature that allows a user account to be automatically created based on the incoming SAML assertion data, if the user does not have an account yet in the tenant's user store. Typically, if the SP federation service fails to map the incoming SAML assertion to a user record, the service collects the data from the assertion and provisions a user record on the fly by using that data.
JSON	JavaScript Object Notation	JavaScript-based data interchange format used as a lightweight alternative to XML.
JWT	JSON Web Token	A claims-based, JSON-formatted security token designed to pass identity information between two parties (similar in use to a SAML assertion).
LDAP	Lightweight Directory Access Protocol	Standard protocol designed to access and maintain user information stored in a directory.

MT	Multi-tenancy	The ability for a (cloud) system to support multiple customers ("tenants") on a single instance of a software application (e.g., SIM or any other OPC service). A tenant includes multiple users. Each tenant in OPC is associated with an identity domain that is a logical identity store hosted in SIM's OID server. All users and groups for the tenant are persisted in this identity store.
OAM	Oracle Access Management	Oracle's access management stack primarily designed for on-premise use. OAM is the foundation technology leveraged by SIM in the cloud.
OAuth	Open Authorization	Delegated, service-to-service authorization standard. SIM also relies on OAuth for identity propagation across Oracle Cloud services.
OID	Oracle Internet Directory	Oracle's LDAP-compliant user directory leveraged by SIM.
OIDC	OpenID Connect	Allows developers to determine the identity of the person using a browser connected to their application. OIDC implements authentication as an extension to the OAuth 2.0 authorization process (OAuth has no notion of identity). Information about the authentication performed is returned to the client in a JWT referred to as an (OIDC) identity token. OIDC is not supported by SIM but will be supported by IDCS. OIDC is comparable to some aspects of SAML usage.
OIF	Oracle Identity Federation	Oracle's legacy, standalone identity federation system whose functionality is now rolled into OAM. OIF is still currently used by Oracle Fusion Applications.
OPC	Oracle Public Cloud	Subscription-based access to Oracle's platform, applications, and social services. OPC is hosted, managed, and supported by Oracle.
PaaS	Platform as a Service	Cloud services allowing developers to build rich applications or extending Oracle SaaS leveraging Oracle Database and WebLogic Server. PaaS services include Java, Documents, Business Intelligence, Mobile, etc.
REST	REpresentational State Transfer	Architecture style for uniformly accessing and modifying a resource (mostly an HTTP API). REST relies on a stateless, client-server, cacheable communications protocol (HTTP). In a REST pattern, you invoke an HTTP method (GET, POST, etc.) on a resource identified by a URL. REST allows for different resource representations (mostly JSON or XML), the client asks for a specific representation through HTTP context negotiation.
SaaS	Software as a Service	Oracle's cloud-based applications including Human Resources, Enterprise Resource Planning, etc.
SAML	Security Assertions Markup Language	Industry-standard, cross-internet domain framework primarily designed to support federated SSO between identity providers and service providers.
SCIM	System for Cross-domain	Industry standard designed to simplify user

	Identity Management	management in the cloud (between identity domains) by defining a schema for representing users and groups and a REST interface to support CRUDQ operations.
SDI	Service Deployment Infrastructure	An integral infrastructure component of Oracle Cloud managing all aspects of runtime provisioning and deployment for a tenant. SDI provides web services to TAS for manipulating identity domains and service instances as well as creation, deletion, up-sizing, and inter-service association. SDI's web services follow the TAS BPEL workflow runtime. TAS is the primary consumer of SDI to manage the business process tracking of all requests from the Oracle Cloud UI portal.
SIM	Shared Identity Management	Current OPC security system, part of OPC's infrastructure (the subject of this document).
SP	Service Provider	In a business partnership, the relying party responsible for consuming standard identity tokens.
SSO	Single Sign-On	Ability for a user to log in once to access multiple web sites without being repeatedly challenged for credentials at each web site in the SSO circle.
TAS	Tenant Automation System	A Java EE application and Oracle Business Process Execution Language (BPEL) Process Manager (PM) application deployed with Oracle Web Services Manager (OWSM) in an Oracle SOA Suite instance. TAS automates all lifecycle operations related to tenant orders and service subscriptions during onboarding (service configuration and activation), scale-up, and termination.
WLS	WebLogic Server	Oracle's Java-based applications container.

Introduction

Shared Identity Management (SIM) is part of Oracle Cloud (OPC). SIM is designed to enable Oracle PaaS services to leverage user authentication, web SSO, inbound identity federation, and web services authorization. Unlike the OPC services shown in the figure below, customers don't subscribe to SIM as SIM is used as an internal component of the OPC security infrastructure.

When a customer (or "tenant") first signs up for an OPC service account, OPC creates an identity domain specific to that customer. When the customer's users log in to an OPC service, the identity domain controls what features they can access (all users are authenticated prior to accessing an application in OPC). Upon activation, OPC automatically assigns the following roles to a customer (the customer may choose to have the same person responsible for one or more roles):

- Account administrator for the service
- Identity domain administrator for the domain
- Service administrator for the service

SIM is designed to control access to other OPC services such as JCS (Java Cloud Service), DOCS (Document Cloud Service), BICS (Business Intelligence Cloud Service), Process Cloud Service (PCS), MCS (Mobile Cloud Service), etc. SIM acts as a service provider (SP) only designed to interoperate with the following identity providers (IdP): Oracle Identity Management 11gR2 PS2, Oracle Identity Federation (OIF) 11gR1 (dedicated to each Oracle Fusion Applications pod), Microsoft Active Directory Federation Services (ADFS) 2.0, 3.0, and 3.1, and Shibboleth 2.4.0.

SIM Functionality

- Administration:
  - Admin password reset user interfaces
  - User/role administration
  - Self service configuration of one external SAML 2.0 Identity Provider (SIM 3.1 only)
  - Self service configuration of OAuth 2.0 clients and resource servers (SIM 3.1 only)
- End-user self service

    - Password reset
- Access Management
    - Authentication against OPC's identity store and single sign-on (SSO) among OPC PaaS services
    - Federated SSO between an external SAML Identity Provider and OPC's PaaS services (SIM 3.1)
    - OAuth-based service-to-service authorization (SIM 3.1 only)
    - OAuth-based identity propagation across services (SIM 3.1 only)
- Identity Store
    - Identity store for users and groups in an identity domain.
- Policy Store
    - Repository for keys, credentials, and policy artifacts (separate from the identity store)
- Utilities
    - Set of multi-tenant scripts for tenant on-boarding

SIM Business Benefits

- Leverage OPC's PaaS services transparently without having to own and deploy software products. No infrastructure administration, upgrade, or migration hassles.
- Enable integration between the customer's (on-premise) identity provider and OPC's PaaS services.
- Bring users, services, and applications together in a secure single point of administration.
- Securely associate OPC's PaaS with SaaS (Oracle Fusion Applications and other Oracle properties).

SIM Releases and Rollout Schedule

As of August 2015, the current release is SIM 3.0. However, SIM 3.1 is now available and is incrementally rolled out in several Oracle data centers (e.g., Chicago, Austin, Sydney, Singapore, Munich, etc.) with support for disaster recovery (see roadmap for updated information on data center rollouts). SIM 3.0 and SIM 3.1 instances will co-exist during full-blown transition to SIM 3.1.

SIM 3.0 Scope

- Local log-in (form-based and basic authentication) and SSO service for Oracle PaaS properties (DOCS, PCS, MCS, JCS) using WebGates (no federation involved).
- SIM as SAML Service Provider to Fusion Applications' SAML Identity Provider via OPC support.

SIM 3.1 Scope

- SIM (as SAML Service Provider) federation with SAML Identity Providers such as Fusion Applications, Oracle Access Management (OAM), Microsoft ADFS, and Shibboleth.

- Web SSO across PaaS and SaaS services, e.g., federated SSO across DOCS (SIM as Service Provider) and Fusion Applications (Identity Provider).
- OAuth 2.0 2-legged service-to-service authorization using Client Credentials or Resource Owner flows (see Appendix for details).
- OAuth-based identity propagation across Oracle Cloud services (see Appendix for details).
- OAuth client management (self service UI + API).
- Self-service SSO setup for using one external Identity Provider.
- Support for OPC's PaaS-SaaS association (see Appendix for details).

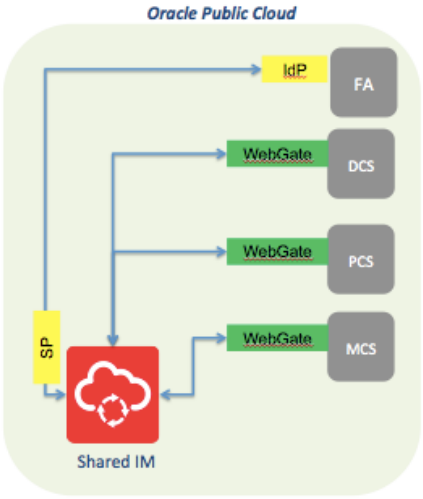
Out of 3.x Scope

- Support for SIM 3.x as an Identity Provider.
- Support for multiple external Identity Providers.
- Support for multi-factor and step-up authentication.
- Support for fraud detection.
- Support for fine-grained authorization.
- 3-legged OAuth support (Authorization Code grant type flow).
- Automated synchronization between the Identity Provider's identity store and SIM's identity store (bulk load only).
- Just-in-time (JIT) user account provisioning.

SSO and Federation Use Case Scenarios

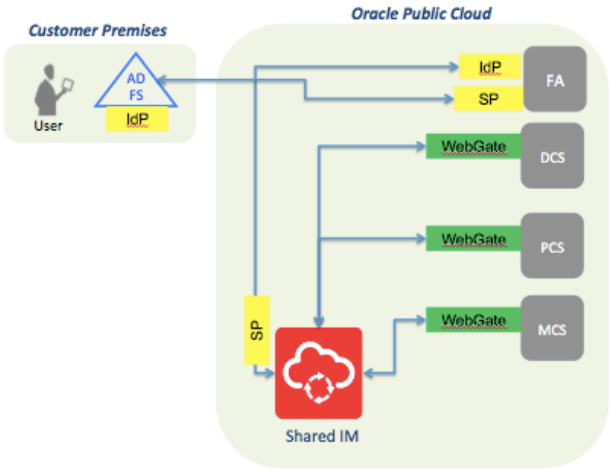
Following are high-level SSO and federation use case scenarios for SIM 3.0 and 3.1.

SIM as Service Provider, Fusion Applications as Identity Provider (*SIM 3.0*)



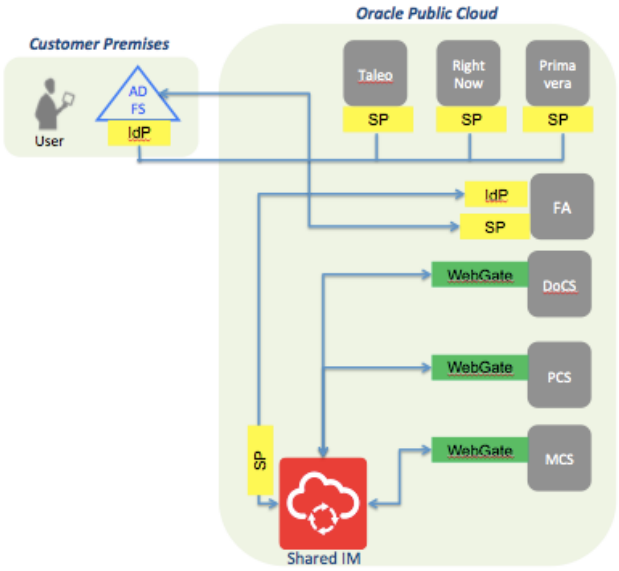
- SIM provides a login service to DOCS, PCS, and MCS via WebGate (WebGate is the web-server-based policy enforcement point for Oracle Access Management)
- Fusion Applications uses a dedicated Oracle Access Management stack (including OIF), and acts as an Identity Provider
- SIM acts as a Service Provider and leverages Fusion Applications' dedicated Oracle Access Management stack as the Identity Provider

SIM as Service Provider, Fusion Applications as Service Provider, Microsoft ADFS as Identity Provider (*SIM 3.0*)



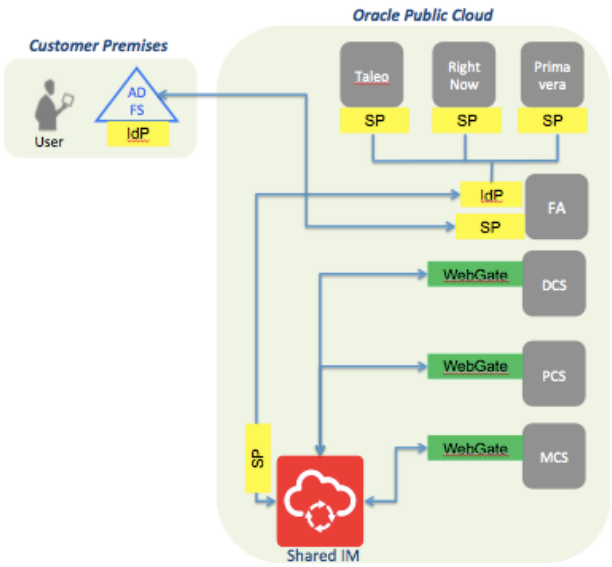
- SIM provides a login service to DOCS, PCS, and MCS via WebGate
- Fusion Applications uses a dedicated Oracle Access Management stack acting as an Identity Provider
- SIM acts as a Service Provider and leverages Fusion Applications' dedicated Oracle Access Management stack as the Identity Provider
- ADFS acts as an Identity Provider to Fusion Applications' Service Provider and Fusion Applications acts as an Identity Provider to SIM (however, in this case, there is no explicit SP/IdP trust between SIM and ADFS: SIM→ FA → ADFS)

SIM as Service Provider, Fusion Applications as Identity Provider and Service Provider, Microsoft ADFS as Identity Provider (*SIM 3.0*)



- SIM provides a login service to DOCS, PCS, and MCS via WebGate
- Fusion Applications uses a dedicated Oracle Access Management stack acting as an Identity Provider to SIM
- SIM acts as a Service Provider and leverages Fusion Applications' dedicated Oracle Access Management stack as the Identity Provider
- Fusion Applications acts as a Service Provider to on-premise Microsoft ADFS Identity Provider
- Oracle's SaaS applications (future) and Fusion Applications act as Service Providers to on-premise ADFS Identity Provider

SIM as Service Provider, Fusion Applications as Identity Provider and Service Provider, Microsoft ADFS as Identity Provider (*SIM 3.0*)

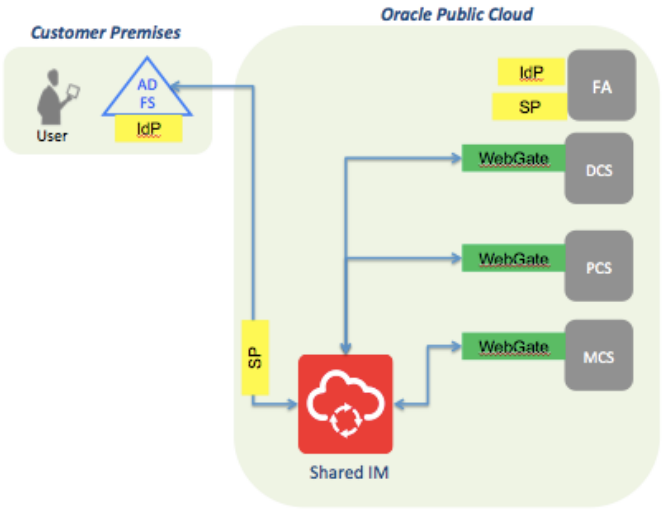


- SIM provides a login service to DOCS, PCS, and MCS via WebGate
- Fusion Applications uses a dedicated Oracle Access Management stack acting as an Identity Provider to SIM
- Fusion Applications acts as an Identity Provider to Oracle's SaaS applications (future)
- SIM acts as a Service Provider and leverages Fusion Applications as the Identity Provider
- Fusion Applications acts as a Service Provider to on-premise Microsoft ADFS Identity Provider
- Oracle's SaaS applications (future) and Fusion Applications act as Service Providers to on-premise ADFS Identity Provider

SIM as Service Provider, Microsoft ADFS as Identity Provider (*SIM 3.1*)

Note1: This use case is also supported by SIM 3.0, however SIM 3.1 adds self-service.

Note2: SIM can act as a Service Provider for only one Identity Provider (either an on-premise ADFS Identity Provider or Oracle Fusion Applications).



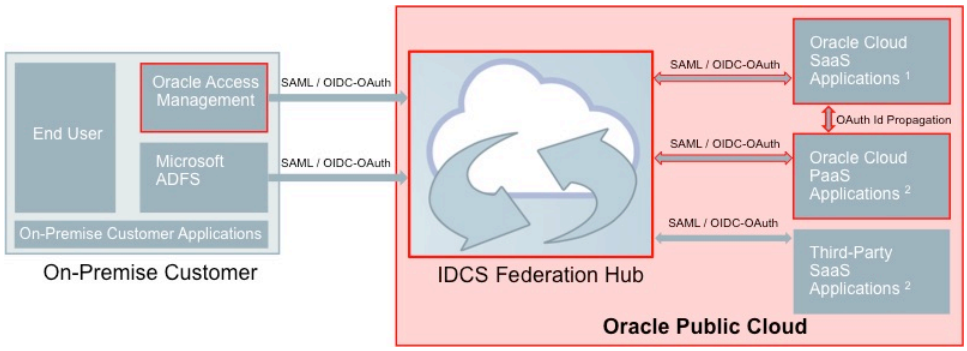
- User logs in to on-premise Microsoft ADFS; ADFS acts as an Identity Provider to SIM
- SIM acts as a Service Provider to ADFS
- SIM provides a login service to DOCS, PCS, and MCS via WebGate

Sneak Preview

Identity Cloud Service (IDCS) will be a new, purpose-built, subscription-based, multi-tenant Oracle Cloud service providing federated SSO and user management functionality for all major Oracle Cloud services as well as Oracle and third-party SaaS applications. IDCS availability date will be communicated later. Unlike SIM, IDCS will be a PaaS identity service offered to customers as well as a service to Oracle Cloud properties. IDCS will eventually replace SIM. There will be a coexistence and migration plan available in the coming months (this plan is outside the scope of this document).

IDCS Use Case (General)

IDCS will provide a federation hub to all Oracle Cloud properties and will bridge on-premise Identity Provider(s) with Oracle Cloud Service Providers. In this case, as a federation hub, IDCS will act both as a Service Provider and Identity Provider.



Note:
([1]) Every OPC property is registered with IDCS as an OAuth client; Each OPC property must identify all its resources to be protected by IDCS.
([2]) The third-party applications hosted by OPC (or hosted by a third-party cloud provider, e.g., Google Apps) must be SAML- and OAuth-enabled.

Summary

Shared Identity Management (SIM) is part of Oracle Cloud. SIM 3.x is designed to enable Oracle PaaS services to leverage user authentication (against a user directory), web single sign-on (SSO) through WebGates, outbound identity federation (SAML 2.0), and service-to-service authorization and identity propagation across services (OAuth 2.0). Unlike other Oracle Cloud services, customers don't subscribe to SIM as SIM is used as an internal component of Oracle Cloud's security infrastructure. Identity Cloud Service (IDCS) will be Oracle Cloud's next-generation identity service, built from the ground up as a cloud service and made available not only to Oracle Cloud internal services but also offered to customers for integration with their enterprise applications.

Appendix

This section provides a Security Assertions Markup Language (SAML) and Open Authorization (OAuth) primer in the context of SIM's usage only.

Security Assertions Markup Language

The Security Assertions Markup Language (SAML) is an industry-standard framework for sharing security information on the Internet through XML documents. SAML was originally designed to address the limitations of proprietary, single-domain browser cookies.

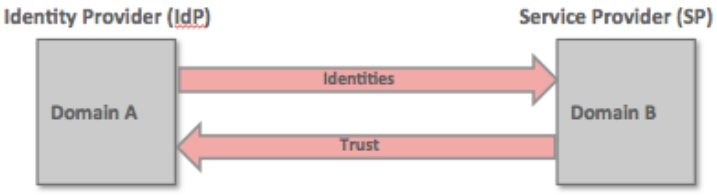
SAML includes 4 parts:

- *Assertions*: How you define authentication information and attribute statements in XML documents.
- *Protocol*: How you ask (SAML Request) and get (SAML Response) the assertions you need.
- *Bindings*: How the SAML Protocol rides on industry-standard transport protocols (e.g., HTTP) and messaging frameworks (e.g., SOAP).
- *Profiles*: How the SAML Protocol and Bindings combine to support specific use cases (e.g., browser profile, artifact profile, etc.).

SAML is the industry's primary solution for federated SSO (or cross-domain SSO) and attribute sharing between interacting parties. Attribute sharing is the ability of a service provider to request user attributes from an identity provider (if necessary) for authentication. SAML does not support fine-grained authorization, which is handled by the Extensible Access Control Markup Language (XACML), outside of SIM's scope.

SAML Concepts

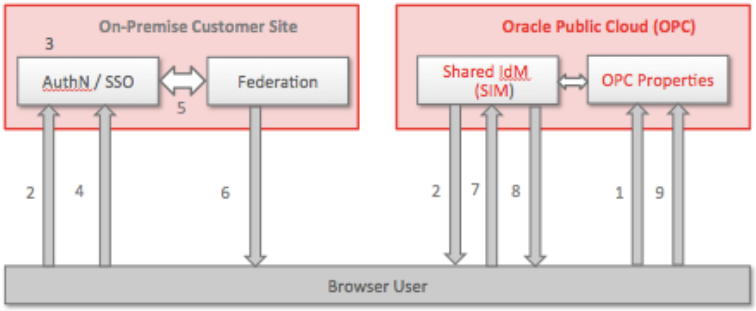
SAML introduces the notion of identity provider and service provider.



The identity provider (IdP) is the asserting party that provides identity information to other services. The IdP generates SAML assertions. The service provider (SP) is the relying party that consumes the SAML assertions sent by the asserting party to grant access to services hosted by the SP. SIM 3.x only acts as a relying party (service provider).

Canonical SAML Use Case for SIM

In this use case, SIM is the Service Provider, Oracle or select third-parties are the Identity Providers. An interactive browser user clicks on an OPC property and is redirected to the Identity Provider for authentication and federated web SSO. In this use case, the HTTP Redirect binding is used to deliver the SAML authentication request message to the Identity Provider and the HTTP POST binding is used to return the SAML response message containing the assertion to the Service Provider.



1. The user attempts to access an OPC property; the user does not have a valid session (security context) on OPC. SIM saves the requested resource URL.
2. SIM sends an HTTP redirect response to the browser. The location HTTP header contains the IdP's SSO service URL together with an authentication request message encoded as a URL query variable.
3. The IdP's SSO service determines whether the user has an existing logon security context at the IdP that meets the authentication request requirements; if not, the IdP interacts with the browser to challenge the user for valid credentials.
4. The user provides credentials and a local logon security context is created for the user at the IdP.
5. The IdP's SSO service generates a SAML assertion representing the user's logon security context. Since in this case the POST binding is used, the assertion is digitally signed and then placed within a SAML response message; the response message is then inserted in an HTML FORM as a hidden form control.
6. The IdP's federation service sends the HTML form back to the browser in the HTTP response (the HTML FORM typically has script code that automatically POSTs the form to OPC's SIM).
7. The browser (either through user action or execution of a script) issues an HTTP POST request to send the form to SIM's assertion consumer service (ACS).
8. SIM performs an access check to ensure that the user is entitled to the OPC property.
9. If the access check passes, the user is logged in and can access the OPC property.

The following Identity Providers (one at a time) are supported by SIM:

- Oracle Access Management Federation 11gR2 PS2
- Oracle Identity Federation 11gR1 (specific to Oracle Fusion Applications pods)
- Microsoft Active Directory Federation Service (ADFS) 2.0, 3.0, 3.1
- Shibboleth 2.4.0

SIM 3.x can only act as a Service Provider and only use web browser profiles (for simplicity). In addition, SIM only provides support for SAML 2.0. If an Identity Provider uses SAML 1.1, for example, the interaction will not be possible (SAML 2.0 and 1.1 XML schemas are not compatible).

Before starting interaction between SIM and a supported Identity Provider, SIM needs the Identity Provider's metadata. SAML 2.0 metadata is the information used for the establishment of trust between federated partners through a standard, interoperable metadata format (XML file). For example, the certificates used for signature and encryption operations are published via the SAML 2.0 metadata file. If ADFS or any other SIM-supported Identity Provider is the customer's on-premise Identity Provider, SIM allows one to obtain that Identity Provider's metadata through a URL. That metadata file is then saved in SIM's environment and used for SIM's configuration.

SAML for PaaS-SaaS Association (SIM 3.1 only)

When a customer purchases both Oracle Fusion Applications (SaaS) and an OPC PaaS service, e.g., Java Cloud Service (JCS), the OPC infrastructure links the two environments via an association process. There is a need for automatic SSO at runtime between the two environments so that the user is challenged for credentials only once. SAML-based federated SSO is used to propagate the user's authentication state from one environment to the other. In this case, Oracle Fusion Applications uses its dedicated federation service (OIF) as the Identity Provider and PaaS federation (SIM) acts as the Service Provider. Two use cases are supported (directly or through redirect):

- The user requests access to a Fusion Applications resource first, and then accesses a PaaS resource.
- The user requests access to a PaaS resource first, and then accesses a Fusion Applications resource.

As mentioned previously, however, SSO among PaaS services only does not require federation and is achieved using WebGate interceptors.

Open Authorization (OAuth)

OAuth is an industry standard designed to support delegated authorization. In OPC, OAuth is used to secure access to exposed PaaS and SaaS properties by implementing service-to-service authorization. Typically, an OPC customer's administrator can protect access to the OPC PaaS and SaaS services his company has subscribed to as well as interactions between on-premise and OPC properties. SIM

3.1 leverages Oracle Access Management's OAuth service to secure REST interactions between services thus eliminating the use of passwords in service-to-service communications and centralizing trust management between (OAuth) clients and servers.

OAuth Concepts

OAuth was originally designed to allow a user (Resource Owner) to transparently share his private data stored on one site (Service Provider, or Resource Server) with another site (Consumer, or Client). With the advent of OAuth 2.0, the original consumer-centric delegated authorization use case extends to the enterprise and the cloud.

OAuth 2.0 enables a third-party application to obtain access on its own behalf (two-legged process) or obtain limited access to an HTTP service on behalf of a Resource Owner by orchestrating an approval interaction between the Resource Owner and the HTTP service provider (three-legged process). SIM 3.1 only provides support for two-legged process flows.

OAuth in OPC

SIM 3.1's OAuth 2.0 authorization service leverages the following OAuth roles:

- Resource Owner: An entity capable of granting access to a protected resource. The resource owner is a person or an application that owns the data to be shared. When the resource owner is a person, it is referred to as an end-user.
- Resource Server: The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens. In Oracle Cloud, the resource server represents an application hosting REST services used by clients, for example Mobile Cloud Service (MCS).
- Client: An application making protected resource requests on behalf of the resource owner and with its authorization. The term client is not specific to a particular entity, for example the client could be an application that executes on a server or mobile device. In Oracle Cloud, the client represents an application making a REST API call like a mobile app or Java Cloud Service application.
- Authorization Server: The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization. In Oracle Cloud, SIM's OAuth Service takes on this responsibility.

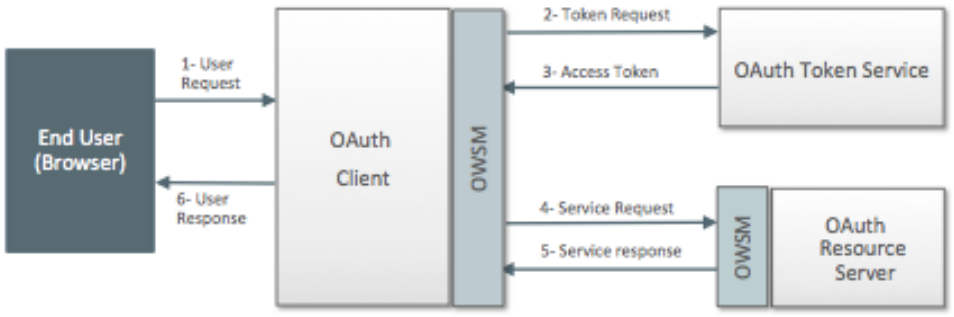
OAuth Token Acquisition Process Flow (2-Legged)

SIM 3.1 protects access to the following OPC properties:

- SaaS applications, e.g., Oracle Fusion Applications, Taleo, Primavera, etc.
- PaaS applications, e.g, JCS, MCS, etc.

On-premise customer or partner applications as well as mobile applications communicate with OPC's properties through REST APIs. SIM 3.1 allows service-to-service authorization among OPC properties and other applications (see Oracle Cloud OAuth Developer's Guide for more information).

The following components are involved in a 2-legged OAuth process:



- *OAuth Client*: An application (e.g., MCS or JCS).
- *OAuth Token Service*: A token issuance end-point that validates client credentials and issues a token to the client. OPC leverages SIM/OAM to provide that service.
- *OAuth Resource Server*: An application hosting REST services used by clients (e.g., MCS).
- *Access Token*: A digitally signed JSON Web Token (JWT) with limited time validity and scope used to represent a client or an end user.
- *Token Request*: A REST API call made by the OAuth Client to the OAuth Token Service to obtain an Access Token.
- *Access Token Response*: Response by the OAuth Token Service containing an Access Token.
- *Service Request*: A REST API call made by the OAuth Client to the OAuth Resource Server.
- *Service Response*: Response from the OAuth Resource Server to a service request (access to resource is now granted).
- Oracle Web Services Manager (OWSM) passes information between the OAuth Client and the OAuth Resource Server; the information includes a client token (containing the client's identity) and a user token (containing the end user's identity); both tokens are signed using the client's tenant private key.

Note: OAuth 2.0 does not provide authentication (this will be supported in IDCS through the OpenID Connect (OIDC) standard). With SIM 3.1, the OAuth Client collects (out of band) and posts end-user credentials to the OAuth Token Server to obtain the OAuth Access Token on behalf of a user. OAuth Client configuration is explained in the Oracle Cloud OAuth Developer's Guide.

Identity Propagation Using OAuth

Typically, when an Oracle Cloud service, e.g., Mobile Cloud Service (MCS), invokes another service, e.g., Fusion Applications, MCS issues a REST call on-behalf of a user in the current Oracle Cloud security context. In this case, MCS does not know the user's credentials. However, a client (e.g., MCS) defined by the customer (or tenant) administrator as "trusted" is entitled to assert a user's identity on behalf of that user. The OAuth Token Service (SIM) acts as the central trust broker between the client (MCS in this case) and the OAuth Resource Server. As a trusted client, MCS propagates the user's identity by generating a signed JWT assertion sent as part of a request to acquire an OAuth Access Token. The OAuth Resource Server verifies that the client is trusted, maps the user assertion's issuer to the client, and validates the user assertion using the client's public key thus achieving service-to-service identity propagation. After validation, the OAuth Token Service provides the client with the access token, which the client presents to the OAuth Resource Server.