Toyota Enterprise Security Service (“TESS”)

Federation Cookbook

Version 1.2

Approvals

Signing of this document acknowledges your concurrence with the validity and accuracy of the information contained in this document.

| **ID** | **Date** | **Name, Department** | **Approval** |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

Revision History

This section represents the change history of the document. All revisions of the document must be tracked by identifying a new version number, the date it was modified, the person making the change, and the reason for the change.

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 11/04/2011 | 1.0 | Initial Draft | Deloitte & Touche |
| 8/20/2014 | 1.1 | Updated for federation services | Deloitte & Touche |
| 12/31/2014 | 1.2 | R2 Upgrade changes | Deloitte & Touche |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc396473733)

[1.1 Purpose 4](#_Toc396473734)

[1.2 Scope 4](#_Toc396473735)

[1.3 References 4](#_Toc396473736)

[1.4 Intended audience 5](#_Toc396473737)

[1.5 Assumptions & Dependencies 5](#_Toc396473738)

[2. Federation Key objectives 6](#_Toc396473739)

[2.1 Conceptual TESS Federated ID Solution 6](#_Toc396473740)

[2.2 Key Business Capabilities 7](#_Toc396473741)

[3. Use cases 8](#_Toc396473742)

[3.1 IdP Initiated Identity Federation 8](#_Toc396473743)

[3.2 SP Initiated Identity Federation 10](#_Toc396473744)

[4. Federation Integration 12](#_Toc396473745)

[4.1 Federation Integration Components 12](#_Toc396473746)

[4.2 TESS Federation Components 12](#_Toc396473747)

[4.3 OIF Administrative Integration 13](#_Toc396473748)

[4.4 OIF Authentication Engine 14](#_Toc396473749)

[4.5 TMS Standards for Federation 14](#_Toc396473750)

[4.5.1 Federated SP Interface 14](#_Toc396473751)

[4.5.2 Federated IdP Interface 14](#_Toc396473752)

[4.6 Federation Protocol Profiles 16](#_Toc396473753)

[4.7 SP initiated Signoff from TMS application 19](#_Toc396473754)

[4.8 OSSO configuration 20](#_Toc396473755)

[4.9 Authentication 21](#_Toc396473756)

[4.10 Customized TESS Login for PD Federation 21](#_Toc396473757)

[4.11 Login framework for applications not using OAM TESS login page 22](#_Toc396473758)

[5. Appendix 24](#_Toc396473759)

[5.1 Appendix A — Terms and Definitions 24](#_Toc396473760)

[5.2 Appendix B – Sample SAML artifacts 25](#_Toc396473761)

1. Introduction

Toyota will develop an Integrated Information Security Model using proven risk-based methodology. This iterative and incremental approach allows us to address multiple threads concurrently while reducing risks and increasing quality. The security policies implemented using this methodology can also be set at global or regional levels. It is the responsibility of the local affiliates to adhere to security policy standards; however, affiliates have flexibility to use any product that supports the standards. As part of this Integrated Information Security Model, Toyota Motor Sales (“TMS”) has implemented a Common Federation Framework by first developing standards and design for federation; then by building the infrastructure and services to support federation capabilities.

## Purpose

This document outlines the different standards, practices and approaches used by TMS to participate the North American Federation (“NA Federation”) initiative. TMS will utilize its TESS solution to provide access to its services to identities outside of its enterprise and to allow its identities to access services outside of its enterprise. This enterprise level identity exchange between TMS and the other Toyota Affiliates is the primary premise of the NA Federation initiative. The TESS federation solution enables Toyota Affiliates, as well as business partners to achieve integration in the TMS identity management realm, by providing a mechanism to share identity information across the respective security domains.

## Scope

This document is limited to industry wide standards in implementing federation services as a part of the TESS solution. It does not list the operational or configurationally information of any specific vendor product. This document provides synopsis of different approaches to implement federation solutions which will facilitate making key architectural decisions.

## References

This document is developed based on implementation experience and generally available documents (regarding the standards, protocols, etc.) including:

* Oracle Identity and Access Management (“IAM”) Resource Library <http://www.oracle.com/us/products/middleware/identity-management/059296.html>
* “Authentication Context for the Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (“SAML”) V2.0”, OASIS Standard, 15 March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>
* “Assertions and Protocol for the OASIS SAML V2.0”, OASIS Standard, 15 March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
* Extensible Markup Language(XML) Schema Part 2: Datatypes Second Edition, W3C. http://www.w3.org/TR/xmlschema-2
* XML – Encryption Syntax and Processing, W3C Recommendation, 10 Dec 2002. http://www.w3.org/TR/xmlenc-core/
* XML – Signature Syntax and Processing, W3C Recommendation, 12 Feb 2002. http://www.w3.org/TR/xmldsig-core/
* Federal Identity Credential and Access Management (FICAM) SAML 2.0 Web Single Sign-On (“SSO”) Profile Version 1.0 http://www.idmanagement.gov/documents/SAML20\_Web\_SSO\_Profile.pdf
* SAML 2.0
* Security and Privacy Considerations for OASIS SAML V2.0 (<http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>)

## Intended audience

This document is intended for consumption by the following roles for the TESS integration and application teams, as well as by Affiliate teams:

* Application Lead
* Application Business Analyst
* Application Architect
* TESS Integration lead
* TESS Business Analyst
* TESS Architect

## Assumptions & Dependencies

* Approval of this document by the Application Lead signifies application team approval to move forward with integration.

1. Federation Key objectives

The following are the key objectives of TESS solution supporting Identity federation.

* Support functionality for the TESS solution to authenticate and federate identities across domains as an Identity Provider (“IdP”) in order to access external services.
* Support Functionality for TESS solution as a Service Provider (“SP”) to externally authenticated users federating into TESS Environment to utilize TESS resources.
* Utilize and support SAML 2.0 protocol.
* Provide functionality for Single Sign-on and Single Sign-off across domains and realms.
* Utilize centralized identity data store maintained by TESS.
* Provide functionality to authorize and authenticate users for access to integrated applications.
* Provide functionality for application areas to utilize existing Fedlet deployments
* Provide High Availability deployment of federation solution

## Conceptual TESS Federated ID Solution

The TESS program aims to provide key AM solution services (e.g. Authentication, Authorization, and Audit) across the enterprise. As a portion of the TESS implementation to simplify authentication and authorization of users accessing applications across domains, a circle of trust is created amongst participating domains to share identity information and decrease the burden of maintenance of each for this identity information.

The TESS federation solution will improve user experience by seamlessly allowing users to transition across domains using SSO and single-sign-off, as part of NA Federation initiative. TMS will act as both an SP for external users to utilize TMS’s resources and as an IdP to federate internal users to use services in other affiliate domains. This federation service will enable users to authenticate and use authorized resources without the need to enter application credentials multiple times. User identity will be federated, and sessions will be managed to enable single sign on and single sign off across realms. SAML 2.0 protocol will be leveraged to facilitate this functionality

Oracle Identity Federation (“OIF”) is a component in the Oracle IAM suite of products that will allow TMS to federate with other entities. OIF comes as a service with R2 version of Oracle Access Management and the service can be enabled/disabled from OAM administration console. TMS has emerging requirements regarding federation where it will look to federate user identity and user sessions to access external applications without having the need to maintain localized, application specific identity stores

In federation, there are two potential roles that an entity can play: IdP and SP. TESS will be leveraged to play both of these roles for TMS, given the nature of its business and relationships with other affiliates and business entities.

When a registered user wishes to access a protected resource in the federated network, the third party SP for that resource directs the user to OIF, which acts as IdP for authentication. OIF would use OAM as an authentication engine to obtain credentials and authenticate the user. OIF can now assert the user's identity to the third party resource (SP), which authenticates the user and provides the requested application.

A third party user including the affiliates tries to access a TMS resource protected by an authentication engine within the TESS framework, such as Oracle Access Manager (“OAM”), which redirects the user to OIF. In an SP role, OIF redirects the user to an IdP such as a portal for global authentication. The IdP portal can now obtain credentials, authenticate the user, and redirect back to OIF, which then retrieves the asserted identity from the IdP. OIF redirects the (authenticated) user to the authentication engine, which grants access to the protected resource.

A unique mapping attribute (TMSFederationLink) attribute will be populated for existing TESS users and provided to the IdPs. The TMSFederationLink attribute is mapped to the corresponding attribute at IdP site to establish account linking Federation between SP and IdP systems.

OIF is a component in the TESS Suite of tools that will allow TESS to federate with other entities. TESS has emerging requirements regarding federation where it will look to federate user identity and user sessions to access external applications without having the need to maintain localized, application specific identity stores.

## Key Business Capabilities

* Secure authentication mechanism for cloud-based applications — TESS provides the ability to access cloud-based applications used by TMS employees and contractors.
* Secure authentication mechanism for ICAM-ready applications — Using SAML 2.0, XYZ can assert identities onto Identity, Credential and Access Management (ICAM) SAML 2.0 aware applications.
* Enhances security and privacy of TMS Associates and Contractors identity information — by eliminating the need issuance of more usernames and passwords to access external applications.
* Fosters collaboration — Using federation, employees and contractors can potentially access SAML 2.0 aware applications hosted by other affiliates to share and communicate information.
* Fosters growth and usage of TMS Line of Business (“LOB”) applications — Enabling TESS Federated SP interface allowing non-TMS employees or contractors the ability to access various TMS applications. It also provides a platform for various Toyota affiliates to interact with each other in a secure way without sharing/duplicating their identities outside of the service domain.
* Reduces costs by reducing user administration costs – Enabling TESS Federated SP services provides TMS the opportunity to sunset existing external user administrations systems used to support external users

1. Use cases

When a registered TMS user wishes to access a protected resource in the federated network, the third party SP along with the services hosted on other Toyota affiliates, for that resource directs the user to OIF, which acts as IdP for authentication. OIF would use OAM as an authentication engine to obtain credentials and authenticate the user. Oracle Identity Federation can now assert the user's identity to the third party resource (SP), which authenticates the user and provides the requested application.

An affiliate user tries to access a TMS resource protected by an authentication engine (OAM) within the TESS framework, which redirects the user to OIF. In a SP role, OIF redirects the user to an IdP such as a portal for global authentication. The IdP portal can now obtain credentials, authenticate the user, and redirect back to OIF, which then retrieves the asserted identity from the IdP. OIF redirects the (authenticated) user to the authentication engine, which grants access to the protected resource.

The two use cases supported by the TESS Federation services are:

* IdP Initiated or
* SP or Relying Party (”RP”)

## IdP Initiated Identity Federation

This is considered an unsolicited transaction because the SP does not request an assertion. Only Hypertext Transfer Protocol (HTTP) Post binding is used.

When a federation request initiated at the IdP, the user is federated to an SP, authenticating the identity to access and utilize applications across domains or realms.

|  |  |
| --- | --- |
| 1. End user visits IdP Web Site and authenticates to the IdP. |  |
| 2. Upon successful authentication, IdP presents end users with a list of trusted SP’s |  |
| 3. End user selects an SP from the list of trusted SP’s presented by the IdP. The IdP then redirects the end user to the SP with an unsolicited SAML assertion. |  |
| 4. SP Verifies SAML Assertion.  SP verifies the Assertion returned by the IdP. SP then provides end users with appropriate access ( In this case , permissions to access the desired SP resources) |  |

## SP Initiated Identity Federation

The SP requests an assertion from the IdP. The SP request uses the HTTP Redirect binding, while the IdP response uses the HTTP Post binding.

|  |  |
| --- | --- |
| 1. End user visits SP web site. SP presents end user with a list of trusted IdP’s. |  |
| 2. End User selects an IdP from the list of Trusted IdP’s presented by the SP. The SP then redirects the end user’s browser with a SAML AuthnRequest to the selected IdP. |  |
| 3. End user authenticates to IdP. IdP provides a SAML response along with mapping attribute (TMSFederationLink) attribute to the SP and redirects the end user back to the SP. |  |
| 4. SP Verifies the Response/ Assertion and for the existences of mapping attribute (TMSFederationLink) attribute in TESS Lightweight Directory Access Protocol (LDAP) which is returned by the IdP. SP then provides end user with appropriate access ) In this case , permission to access the desired SP resources) |  |

1. Federation Integration

Toyota has embarked in implementing federation solutions that will be tightly integrated with TESS components for IAM. As an IdP, the primary authoritative source for user information will be obtained from TESS. Active and authorized user information from TESS will be used to create federation protocols within the circle of trust domains to federate users.

## Federation Integration Components

The TMS OIF implementation will leverage the other components of the TESS infrastructure for tighter integration with existing IAM components

The components utilized for successful setup of OIF at TMS will include

1. Oracle Identity Manager (“OIM”)**:**  This will be utilized for the creating and maintaining User Identities across TESS infrastructure.
2. Oracle Directory Server Enterprise Edition (“ODSEE”)**:** The ODSEE will be the primary source as an LDAP directory for obtaining user attributes and entitlements for OIF as an IdP and a SP.
3. Oracle Virtual Directory (“OVD”): OIF will point to the virtual directory for obtaining user identity, primarily from ODSEE. Should a user exist in the primary source, OVD will gather user attributes to other sources through a join view adapter.
4. Oracle Access Manager (“OAM”): OAM will protect defined resources and validate user access based on predefined attributes and access rules defined in the ODSEE or other defined directory sources.
5. WebGates: WebGates installed in the infrastructure will validate users through OAM, and should the identity not exist, the request will be forwarded to OIF for its capacity to either provide access as an IdP or a SP.

## TESS Federation Components

|  |  |  |
| --- | --- | --- |
| Component | Interface | Description |
| **Presentation Tier** | | |
| Admin Web Interface | HTTP(S) | The administrative interface for OIF that allows for the configuration of OIF and federation policies, etc. The OIF Admin Web Interface is deployed on a separate HTTP server from the OIF Federation Proxy. |
| Federation Proxy | HTTP(S) | An HTTP server which resides in the DMZ and forwards requests and responses to the federation server, enabling transparent access to the server from an external network such as the internet. |
| Oracle OpenSSO Fedlets | Java/.Net | This component is provided as an integration mechanism to provide an existing application a way to “speak SAML” and integrate with an IdP. |
| **Application Tier** | | |
| SP Engine | N/A | The module that creates a local authenticated session for the user based on a received federated SSO token. |
| Authentication Engine | HTTP(S) | The module that challenges users when they log in. |
| Federation Server | HTTP(S) | The policy decision point for OIF where federation policies and OIF configuration are administered (via a web interface). |
| **Data Tier** | | |
| Configuration Data Store | Oracle database (DB) | The repository containing OIF configuration data. |
| Federation Data Store | ODSEE 11g | The repository containing federated user account linking data. |
| User Data Store | ODSEE 11g | The repository containing the identity information of the users the OIF system authenticates. |
| User Session Store and Message Store | Oracle DB | The repository containing transient runtime session state data and protocol messages. |

Table 4.2‑1 Federation Components

## OIF Administrative Integration

Oracle Identity federation integrates with Oracle Fusion Middleware. The integration touch points are

* Oracle HTTP Server for OAM Integration
* Oracle HTTP Server to be set as a proxy for OIF

## OIF Authentication Engine

Most OIF features require the user to be authenticated. These operations include both IdP and SP protocol operations such as SSO, federation creation, federation termination, and NameID registration. The federation server provides support of federation protocol such as Liberty 1.x, SAML 1.0/1.1, and SAML 2.0 protocols. Additionally, the federation authentication module provides support for user authentication and integration with IAM solutions. The OIF’s authentication engine interacts with OAM to provide web SSO. User entitlements are defined based on attributes stored in LDAP.

For IdP initiated authentication requests, a default IdP scheme such as “TMS Authentication” scheme will be set using an online WLST command. This configuration will use the default authentication scheme to be effective for all federation integrations that require IdP initiated authentication.

## TMS Standards for Federation

### Federated SP Interface

The following section defines the Federated SP interface and how IdPs will need to configure their IdP servers to exchange information with SP applications for authentication and authorization.

* + - 1. Interface Definition

The Traditional Federated SP Interface supports the following use cases:

* External TMS vendors or business partners accessing Client XYZ web applications (i.e., also known as Business-to-Business (“B2B”))
* Toyota business affiliate (e.g. TFS, TEMA) end-users accessing Client XYZ web applications (i.e., also known as B2B)
  + - 1. Interface Requirements
* Toyota North American (“NA”) affiliate IdPs requesting to interoperate with the TESS must conform to the OASIS SAML 2.0 Web SSO Profile Version 1.0.
* Toyota NA affiliate IdPs must provide signed SAML 2.0 metadata to the TESS Integration Services Team.
* To obtain a signed TESS SP SAML 2.0 Metadata file please consult your assigned TESS Integration platform Team member.
* IdP must won and operate their own Federated instance (i.e., Federated Identity and Access Management component such as OIF, Rivest, Shamir, & Adleman (RSA) Federated Identity Manager (“FIM”), Computer Associates (CA) SiteMinder, OpenSSO)

### Federated IdP Interface

The following section defines the Federated IdP interface and how SPs will need to configure their applications to exchange information with IdPs for authentication and authorization.

* + - 1. Interface Definition

The Traditional Federated IdP Services support the following use cases:

* Toyota NA affiliate (e.g., TFS, TEMA) employees or contractors accessing TMS owned web applications using TESS web SSO.
* TMS employees or contractors accessing external Client XYZ-owned web applications (e.g., cloud-based SPs, software-as-a-service (“SaaS”) providers, and externally hosted applications) using TESS web SSO.
  + - 1. Interface Requirements for IdPs
* Toyota NA affiliate web application requesting to interoperate with TMS should conform to the OASIS SAML 2.0 Web SSO Profile Version 1.0.
* All affiliates (i.e. SPs) must provide signed SAML 2.0 metadata documents to the TESS Integration platform Team.
* SP must own and operate their own Federated instance (i.e., Federated Identity and Access Management component such as Oracle Identity Federation (OIF)), RSA Federated Identity Manager (FIM), CA SiteMinder, OpenSSO).
  + - 1. Interface Configuration Parameters

This section describes the sample token a SP may consume to support TESS authentication via Federated means. To consume TESS OASIS SAML 2.0 assertions, an application needs to consume the latest SAML 2.0 IdP metadata file signed by the TESS Team. Below is a sample portion of a signed SAML 2.0 IdP metadata file.

Figure 4.5.1 Sample Signed SAML 2.0 IdP Metadata

[**-**](file:///C:/Users/demohanty/AppData/Local/Microsoft/vsundaram/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/A) <md:EntityDescriptor xmlns:md="**urn:oasis:names:tc:SAML:2.0:metadata**" ID="**id-qjp5DLY9-Q1CDNacoC1AjkZABKQ-**" entityID="**http://abctms.toyota.com/fed/IdP**" validUntil="**2011-04-20T14:38:16Z**">

[**-**](file:///C:/Users/demohanty/AppData/Local/Microsoft/vsundaram/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/A) <dsig:Signature xmlns:dsig="**http://www.w3.org/2000/09/xmldsig#**">

[**-**](file:///C:/Users/demohanty/AppData/Local/Microsoft/vsundaram/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/A) <dsig:SignedInfo>

  <dsig:CanonicalizationMethod Algorithm="**http://www.w3.org/2001/10/xml-exc-c14n#**" />

  <dsig:SignatureMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#rsa-sha1**" />

[**-**](file:///C:/Users/demohanty/AppData/Local/Microsoft/vsundaram/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/A) <dsig:Reference URI="**#id-qjp5DLY9-Q1CDNacoC1AjkZABKQ-**">

<dsig:Transforms>

  <dsig:Transform Algorithm="**http://www.w3.org/2000/09/xmldsig#enveloped-signature**" />

  <dsig:Transform Algorithm="**http://www.w3.org/2001/10/xml-exc-c14n#**" />

  </dsig:Transforms>

  <dsig:DigestMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#sha1**" />

  <dsig:DigestValue>x4jl56zYzb3wUc9dvPupmcaHoUc=</dsig:DigestValue>

  </dsig:Reference>

  </dsig:SignedInfo>

  <dsig:SignatureValue>m+Y0FUrCI0/DPzV8jXL3oh3NuunyrjwYVLyhGz2zQe602McQY4w9XqMSa5rTw0hRJOnwUPUTQMRcT4uP3VDPhVONMC19OeFbUgauJAvbxkvKXmdMGf3Jk96YHb0ZVRERV+3QbaMLQDqLkKLWMNbjDsfDpSwXE1Ysf+iA74y5iZM=</dsig:SignatureValue>

[**-**](file:///C:/Users/demohanty/AppData/Local/Microsoft/vsundaram/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/A) <dsig:KeyInfo>

[**-**](file:///C:/Users/demohanty/AppData/Local/Microsoft/vsundaram/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/AppData/Local/Microsoft/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/A) <dsig:X509Data>

  <dsig:X509Certificate></dsig:X509Certificate>

  </dsig:X509Data>

  </dsig:KeyInfo>

</dsig:Signature>

## Federation Protocol Profiles

Federation framework will be setup as an IdP and SP to exchange assertions using profiles and services defined by the federation protocol. Assertion for such identity federation will establish a secure connection, securely authenticate data across the connection and receive interpreting assertion from other SAML domain using the following mechanisms.

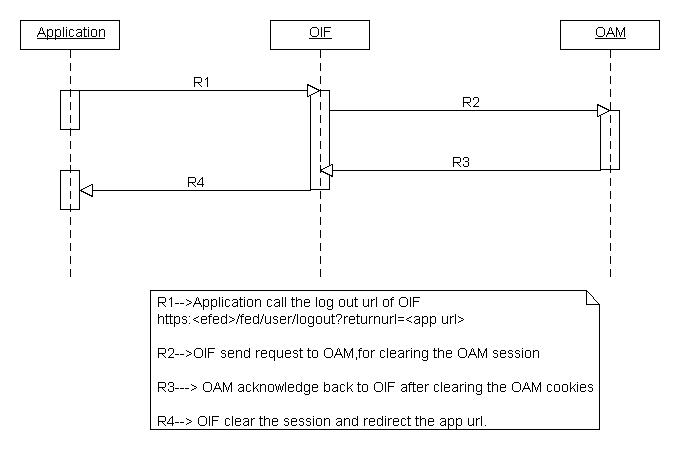
1. Browser POST profile: The SAML Browser POST profile sends a full assertion from an IdP to a SP without the use of an artifact. OIF sends the assertion to the user’s browser as a secure variable in HyperText Markup Language (HTML) form and the browser then posts the assertion to the destination site. HTTP POST binding provides a framework for the embedding and transport of the SAML 2.0 Protocol.
2. Browser Artifact Profile: Due to limitations on browser Uniform Resource Locator (URL) Handling, SAML Browser Artifact profile transmits data using compact reference to an assertion using a reference to an artifact. The recipient of the artifact users the artifact resolution protocol to obtain the full assertion.
3. Simple Object Access Protocol (SOAP) Binding: The Mapping of abstract message exchanges to real messages or communication protocols, also defines SAML Protocol communication within SOAP messages.
4. Browser HTTP Redirect Profile: The Browser HTTP redirect profile indicates to the requesting party of a change in URL. HTTP Redirect binging uses the HTTP Redirect response to send data in URL through the users query string parameters though a user’s browser from one resource to another.
5. Name Identifier Management profile: Name Identifier Management defines provider communication with each other with one of the providers in the circle of trust to update the name identifier assigned to a common shared user. OIF supports these SOAP/HTTP and HTTP-redirect name identifier profiles:

* SAML 2.0 IdP-Initiated Manage NameID Profile for Name Identifier Update
* SAML 2.0 SP-Initiated Manage NameID Profile for Name Identifier Update

1. SAML Attribute Sharing Profile: SAML provides an attribute query / response protocol for retrieving principals attributes. Authentication is achieved by presenting the users federated credentials in the form of a trusted X.509V3certificate, along with the proof of possession of the associated Private Key. If the SP requires additional information about the principal to determine authorization, the Subject Distinguished Name (DN) from this certificate issued to query an IdP for the required attributes.
2. Federation Termination Profile: Users termination in a federation is used by a link on the IdP’s or SP’s domain resource. An initiated request to terminate the user notifies SP or IdP resources for authentication and authorization of this change. Following are the supported termination profiles

* SAML 2.0 IdP Initiated Manage NameID Profile for Name Identifier Deletion
* SAML 2.0 SP Initiated Manage NameID Profile for Name Identifier Deletion

1. Global Logout Profile: When a user initiates a logout the IdP sends each active SP a request to logout for the user.



Sequence diagram: 4.7.0

## Federation attribute profiles

Attribute profiles can be defined for IdP/SP systems using OAM administration privileges where the list of user attributes will be specified which will be transmitted to federated systems. Once defined, these profiles can be re-used for all TESS federation integrations.

## SP initiated Signoff from TMS application

The TESS Federation Management service is configured with SP initiated sign off. This will allow the users, who have logged in using federation, to logoff from TMS application. In this scenario, TESS acts as a SP and the user initiates the logout from TMS application.

When the user clicks on the logout link from the TMS application, the application cleans out the application specific session/cookies, and calls the TESS efed logout URL. TESS efed logout URL deletes the OAM specific cookies, federation session and sends the SAML logout request to IdP.

1. Federated User initiates the logout by clicking on the logout link on the TMS application. The application invalidates the application specific cookie.
2. The logout request is forwarded to the TESS federation SP logout URL. TESS SP invalidates the federated session and internally calls the OAM logout URL to kill the OAM session.
3. OAM invalidates user’s OAM session and redirects back to OIF.
4. OIF invalidates the federation session
5. User is redirected to the configured logout page.

In case the IdP initiates the logout request and needs to invalidate the TESS specific session for the user, the OIF TESS federation logout URL will be configured in IdP to invalidate the TESS specific session.

The below table describes the Federation URL which the application should embed in the application Logout link.

|  |  |
| --- | --- |
| Environment | Logout URL |
| Shared Development Future | https://ssologin-f02.dev.toyota.com/tesslogin/logout?end\_url=https://ssologin-f02.dev.toyota.com/tesslogin/fedLogout.jsp |
| Shared QA Future | https://ssologin-f02.qa.toyota.com/tesslogin/logout?end\_url=https://ssologin-f02.dev.toyota.com/tesslogin/fedLogout.jsp |
| Stage | https://ssologin-stg2.qa.toyota.com/tesslogin/logout?end\_url=https://ssologin-f02.dev.toyota.com/tesslogin/fedLogout.jsp |
| Production | https://ssologin.toyota.com/tesslogin/logout?end\_url=https://ssologin-f02.dev.toyota.com/tesslogin/fedLogout.jsp |



## OSSO configuration

During SP initiated SSO federation pattern for PDs and affiliates, OIF will redirect the user to the OAM Delegated Authentication Protocol (DAP) login URL which will create the DAP token, translate the session and create the OAMAuthnCookie.

A default SP integration module is required to be configured on SP (OIF) and Oracle Single Sign-On (OSSO). The OSSO configuration module requires following details.

Once the user is successfully authenticated by IdP, the IdP sends the SAML assertion to OIF with the required Name-ID format. OIF then consumes the Name-ID and submits a Delegated Authentication Protocol(DAP) request to OAM for creating the OAM session and cookie information.

|  |  |
| --- | --- |
| Parameter | Value |
| Authentication Mechanism | oracle:fed:authentication:password-protected |
| Username Attribute | uid |
| Login URL | https://<sso\_login\_proxy\_url/oam/server/dap/cred\_submit |
| Logout URL | https://<sso\_login\_proxy\_url/oam/server/logout |

## Authentication

Federating users to use external resources requires that such users are successfully authenticated before a resource is available to the user. This operation includes

* IdP protocol operation like SSO, Federation creation, Federation Termination and NameID Registration
* SP Protocol operations such as Federation creation, Federation termination and NameID Registration.

The Authentication engine acts as a local authentication mechanism, the authentication module can authenticate locally with available authentication system. The OIF conveys authentication requests to the authentication module, which interacts directly with user repositories in OID / OVD or rational database management systems (“RDBMS”), or delegate authentication to OAM.

The OIF SP integration engine acts to propagate the authentication state, using federation protocols to have the user authenticated at a peer IdP. OIF forwards the user to the authentication module, which propagates and creates an authenticated user sessions at the SP.

## Customized TESS Login for PD Federation

A framework has been designed with federation SP pattern for allowing PDs and affiliates users to access the TMS application using federated SSO.

The existing standard TESS login page has been customized to have a link that allows PD or affiliate user to access TMS application. User can click on the new link available, which further provides a drop down for the user to select a desired IdP for carrying out the authentication process.

Each IdP in the drop down has a mapped URL which is retrieved from a property file. The mapped URL is used when the user makes the choice for which IdP to authenticate in the drop down.

The drop down URL contains the following three parts:

* 1. SP Federation initiated URL (TESS)
  2. IdP ID
  3. Return URL

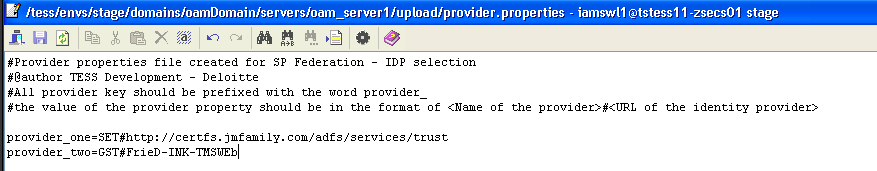
IdP ID is retrieved from the properties file and appended to the SP Federation URL. Return URL is calculated dynamically from the query parameter (resource\_url) of TESS Login page and is appended to the URL as shown below.

*https://<SP HOST>/fed/sp/initiatesso?providerID=<IdP entity ID>&returnurl=<Requested application URL>*

The list of IdPs can be extended as per future requirements by updating the properties file.

|  |  |
| --- | --- |
| Environment | Properties file location |
| DEV FR | /tess/envs/devfr/domains/oamDomain/servers/oam\_server1/upload |
| QA FR | /tess/envs/qafr/domains/oamDomain/servers/oam\_server1/upload |
| Stage | /tess/envs/stage/domains/oamDomain/servers/oam\_server1/upload |
| Production | /tess/envs/prod/domains/oamDomain/oam\_server1/upload |

Sample properties file looks like below,



A separate “Need Help” page has been designed for PD federation to provide guidance to federated user during the time of login.

## Login framework for applications not using OAM TESS login page

All applications which use the custom login page need to make additional changes to enable the user to select the IdP for federated authentication.

The following changes should be made to the existing application specific login pages.

1. Add an additional link on the application login page to re-direct users to IdP selection screen
2. On IdP selection screen, perform code changes to construct SP initiated federation URL based on IdP selection made by the user.

The table below provides the sample code which should be added to the application login page to provide an additional link for PD and affiliate users to choose Identity provider.

|  |
| --- |
| <tr>  <td colspan="2" style="text-align:center;">  <font size=1><span style="color:black;text-wrap:normal;">Private Distributors & Affiliates, <a href="/tesslogin/IdPProvSel.jsp?resource\_url=<%=requested\_url%>" title="Identity Provider Selection Page" target="\_parent">Click here</a></span></font>  </td>  </tr> |

The table below provides the sample code which should be added IdP selection page for PD and affiliate users.

|  |
| --- |
| <tr>  <% String commonURL = "https://efed-stg01.qa.toyota.com/fed/sp/initiatesso?providerid="; %>  <td>  <SELECT id="providerId" NAME="provider" style="width: 100px;">  <option value=""></option>  <%  Properties prop = new Properties();  prop.load(new FileInputStream("/tess/envs/<env>/domains/oamDomain/servers/oam\_server1/upload/provider.properties"));    Enumeration propNames = prop.propertyNames();  while(propNames.hasMoreElements()){  String key = (String) propNames.nextElement();  if(key.startsWith("provider\_")){  String propVal = (String) prop.getProperty(key);  String providerName = propVal.substring(0,propVal.indexOf("#"));  String providerId = propVal.substring(propVal.indexOf("#")+1,propVal.length());  String providerVal = commonURL+providerId+"&returnurl="+requested\_url;  %>  <option value="<%=providerVal%>"><%=providerName%></option>  <%  }  }  %>  </SELECT>  </td>  </tr> |

1. Appendix

This section contains information to supplement the content contained in this document.

## Appendix A — Terms and Definitions

This section defines the terms and definitions required to interpret the document.

|  |  |
| --- | --- |
| **Term** | **Description** |
| OAM | Oracle’s web access management product, a part of Oracle’s Identity and Access Management Suite |
| OIF | Oracle’s Federation product, a part of Oracle’s Identity and Access Management Suite |
| Federation | The security concept of exchanging identity information (authentication and authorization assertions) between security domains |
| SP | SP is an [entity](http://en.wikipedia.org/wiki/Entity) that provides [services](http://en.wikipedia.org/wiki/Service_(economics)) to other entities. |
| IdP | IdP is an authentication module which verifies an identity token, as an alternative to explicitly authorizing a user within a security realm |
| ODSEE | ODSEE is a LDAP V3 standard directory server. It will be deployed as the User store for TESS. |
| OVD | Oracle Virtual Directory provides an aggregated view of various directories and databases. |
| IAM | IAM system  identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. |
| RDBMS | RDBMS stores data in tables and relationships among the data are also stored in tables. |
| SAML | SAML - An XML-based standard for exchanging authentication and authorization data between security domains |
| SaaS | SaaS is a [software](http://en.wikipedia.org/wiki/Software) delivery model in which software and its associated [data](http://en.wikipedia.org/wiki/Data_(computing)) are [hosted](http://en.wikipedia.org/wiki/Internet_hosting_service) centrally |
| LDAP | LDAP is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. |
| SSO | SSO enables the user to [log in](http://en.wikipedia.org/wiki/Log_in) once and gains access to integrated enterprise systems without being prompted tor log in again. |
| WLST | The WebLogic Scripting Tool (WLST) is a command-line scripting interface that system administrators and operators use to monitor and manage WebLogic Server instances and domains. |

Table 5.1‑1 Terms and Definitions

## Appendix B – Sample SAML artifacts

Figure below provides a sample artifact of SAML 2.0 responses, assertions, and subjects.

Figure 5.2.1

Figure 5.2.2 Sample SAML 2.0 Response

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="id-1gXJGzPOGdGXrnX0WGrT5v9XFrY-" Version="2.0" IssueInstant="2011-03-16T17:56:44Z" Destination="[http://abctms12.toyota.com:7001/fedletsample/fedletapplication](http://kcgams12.gsa.gov:7001/fedletsample/fedletapplication)"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">[http://abctms16.xyz.com/fed/IdP](http://kcgams16.gsa.gov/fed/idp)</saml:Issuer><samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">  
<samlp:StatusCode  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"  
Value="urn:oasis:names:tc:SAML:2.0:status:Success">  
</samlp:StatusCode>  
</samlp:Status><saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="id-JEFqQjhEKadXLEFK40EsWWYNmqs-" IssueInstant="2011-03-16T17:56:44Z" Version="2.0"><saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">[http://abctms16.xyz.com/fed/IdP](http://kcgams16.gsa.gov/fed/idp)</saml:Issuer><dsig:Signature xmlns:dsig="[http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig)"><dsig:SignedInfo><dsig:CanonicalizationMethod Algorithm="[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)"/><dsig:SignatureMethod Algorithm="<http://www.w3.org/2000/09/xmldsig#rsa-sha1>"/><dsig:Reference URI="#id-JEFqQjhEKadXLEFK40EsWWYNmqs-"><dsig:Transforms><dsig:Transform Algorithm="<http://www.w3.org/2000/09/xmldsig#enveloped-signature>"/><dsig:Transform Algorithm="[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)"/></dsig:Transforms><dsig:DigestMethod Algorithm="<http://www.w3.org/2000/09/xmldsig#sha1>"/><dsig:DigestValue>NT9WqFZQqv4d5RxxZb4baqs15EI=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>n+qxW4I72z0gAww2J+1bKw/s/GuVy+1SeUJLrpmx4gnakmnxaXlLKjUk43JaT396CHNfS7DS8DjWXd91jKHKBWxnSBQB+wWFd4jqZHpm9XtgTiDwCzTnh44xVwF0d7ihPXZYQ13n0OvdxQ7qJS+XsWb2eAVyRgBNhAM3MkZBa38=</dsig:SignatureValue></dsig:Signature><saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="[http://abctms16.xyz.com/fed/IdP](http://kcgams16.gsa.gov/fed/idp)" SPNameQualifier="fedlet\_sp\_sample">id-36u3C-g0WzfNC0foAP4lUb9fY-w-</saml:NameID><saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData NotOnOrAfter="2011-03-16T18:11:44Z" Recipient="[http://abctms12.toyota.com:7001/fedletsample/fedletapplication](http://kcgams12.gsa.gov:7001/fedletsample/fedletapplication)"/></saml:SubjectConfirmation></saml:Subject><saml:Conditions NotBefore="2011-03-16T17:46:44Z" NotOnOrAfter="2011-03-16T18:11:44Z"><saml:AudienceRestriction><saml:Audience>fedlet\_sp\_sample</saml:Audience></saml:AudienceRestriction></saml:Conditions><saml:AuthnStatement AuthnInstant="2011-03-16T17:56:43Z" SessionIndex="id-TBR9mdG0IkDZf0RwyA-kPZc6OBA-" SessionNotOnOrAfter="2011-03-16T18:56:44Z"><saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement><saml:AttributeStatement xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500" xmlns:xs="<http://www.w3.org/2001/XMLSchema>" xmlns:xsi="<http://www.w3.org/2001/XMLSchema-instance>"><saml:Attribute Name="MName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/><saml:Attribute Name="FNAME" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">John</saml:AttributeValue></saml:Attribute><saml:Attribute Name="Email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">[john.doe@xyz.com</saml:AttributeValue></saml:Attribute><saml:Attribute](mailto:john.doe@gsa.gov%3c/saml:AttributeValue%3e%3c/saml:Attribute%3e%3csaml:Attribute) Name="UPN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">[0123456789@xyz.com</saml:AttributeValue></saml:Attribute><saml:Attribute](mailto:0123456789@xyz.gov%3c/saml:AttributeValue%3e%3c/saml:Attribute%3e%3csaml:Attribute) Name="Organization" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/><saml:Attribute Name="UserID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">47001000654321</saml:AttributeValue></saml:Attribute><saml:Attribute Name="SN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Doe</saml:AttributeValue></saml:Attribute><saml:Attribute Name="FASCN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">47000003210465444000567890147005</saml:AttributeValue></saml:Attribute><saml:Attribute Name="Agency" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/></saml:AttributeStatement></saml:Assertion></samlp:Response>

Figure 5.2.3 Sample Subject

<saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
<saml:NameID NameQualifier="http://abctms.toyota.com /fed/IdP" SPNameQualifier="fedlet\_sp\_sample" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">id-36u3C-g0WzfNC0foAP4lUb9fY-w-</saml:NameID><saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">  
<saml:SubjectConfirmationData NotOnOrAfter="2011-03-16T18:11:44Z" Recipient="[http://abctms12.toyota.com:7001/fedletsample/fedletapplication](http://kcgams12.gsa.gov:7001/fedletsample/fedletapplication)" ></saml:SubjectConfirmationData></saml:SubjectConfirmation>  
</saml:Subject>

Figure 5.2.4 Sample Assertion

<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="id-JEFqQjhEKadXLEFK40EsWWYNmqs-" IssueInstant="2011-03-16T17:56:44Z" Version="2.0"><saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">[http://abctms16.toyota.com/fed/IdP](http://kcgams16.gsa.gov/fed/idp)</saml:Issuer><dsig:Signature xmlns:dsig="[http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig)"><dsig:SignedInfo><dsig:CanonicalizationMethod Algorithm="[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)"/><dsig:SignatureMethod Algorithm="<http://www.w3.org/2000/09/xmldsig#rsa-sha1>"/><dsig:Reference URI="#id-JEFqQjhEKadXLEFK40EsWWYNmqs-"><dsig:Transforms><dsig:Transform Algorithm="<http://www.w3.org/2000/09/xmldsig#enveloped-signature>"/><dsig:Transform Algorithm="[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)"/></dsig:Transforms><dsig:DigestMethod Algorithm="<http://www.w3.org/2000/09/xmldsig#sha1>"/><dsig:DigestValue>NT9WqFZQqv4d5RxxZb4baqs15EI=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>n+qxW4I72z0gAww2J+1bKw/s/GuVy+1SeUJLrpmx4gnakmnxaXlLKjUk43JaT396CHNfS7DS8DjWXd91jKHKBWxnSBQB+wWFd4jqZHpm9XtgTiDwCzTnh44xVwF0d7ihPXZYQ13n0OvdxQ7qJS+XsWb2eAVyRgBNhAM3MkZBa38=</dsig:SignatureValue></dsig:Signature><saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="[http://abctms16.toyota.com/fed/IdP](http://kcgams16.gsa.gov/fed/idp)" SPNameQualifier="fedlet\_sp\_sample">id-36u3C-g0WzfNC0foAP4lUb9fY-w-</saml:NameID><saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData NotOnOrAfter="2011-03-16T18:11:44Z" Recipient="[http://abctms12.toyota.com:7001/fedletsample/fedletapplication](http://kcgams12.gsa.gov:7001/fedletsample/fedletapplication)"/></saml:SubjectConfirmation></saml:Subject><saml:Conditions NotBefore="2011-03-16T17:46:44Z" NotOnOrAfter="2011-03-16T18:11:44Z"><saml:AudienceRestriction><saml:Audience>fedlet\_sp\_sample</saml:Audience></saml:AudienceRestriction></saml:Conditions><saml:AuthnStatement AuthnInstant="2011-03-16T17:56:43Z" SessionIndex="id-TBR9mdG0IkDZf0RwyA-kPZc6OBA-" SessionNotOnOrAfter="2011-03-16T18:56:44Z"><saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement><saml:AttributeStatement xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500" xmlns:xs="<http://www.w3.org/2001/XMLSchema>" xmlns:xsi="<http://www.w3.org/2001/XMLSchema-instance>"><saml:Attribute Name="MName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/><saml:Attribute Name="FNAME" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">John</saml:AttributeValue></saml:Attribute><saml:Attribute Name="Email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">[john.doe@toyota.com</saml:AttributeValue></saml:Attribute><saml:Attribute](mailto:john.doe@gsa.gov%3c/saml:AttributeValue%3e%3c/saml:Attribute%3e%3csaml:Attribute) Name="UPN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">[0123456789@toyota.com </saml:AttributeValue></saml:Attribute><saml:Attribute](mailto:0123456789@xyz.gov%20%3c/saml:AttributeValue%3e%3c/saml:Attribute%3e%3csaml:Attribute) Name="Organization" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/><saml:Attribute Name="UserID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">47001000654321</saml:AttributeValue></saml:Attribute><saml:Attribute Name="SN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Doe</saml:AttributeValue></saml:Attribute><saml:Attribute Name="FASCN" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">47000003210465444000567890147005</saml:AttributeValue></saml:Attribute><saml:Attribute Name="Agency" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/></saml:AttributeStatement></saml:Assertion>