HP Select Federation

For the HP-UX, Linux, Solaris and Windows® operating systems

Software Version: 7.00

Deployment Concepts Guide

Document Release Date: August 2007
Software Release Date: September 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

HP Select Federation includes software developed by third parties. The software in Select Federation includes:

- Apache Derby, Apache Xalan Library, Apache Xerces Library, and Apache XML Dsig Library.
- Software developed by the Waveset Technologies, Inc. (www.waveset.com).
- Software developed by the University Corporation for Advanced Internet Development <http://www.ucaid.edu>Internet2 Project.

Trademark Notices

- Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
- Microsoft®, Windows®, and Windows XP® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation.
- UNIX® is a registered trademark of The OpenGroup.

Documentation Updates

This manual's title page contains the following identifying information:

- Software Version number, which indicates the software version
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Introduction

About This Guide

This *HP Select Federation Deployment Concepts Guide* is intended to help you plan a Select Federation deployment. This guide helps customers start a federation project with Select Federation and take it to a successful deployment in real production environments.

Who This Guide is For

This guide is intended for customers or field personnel who are responsible for taking a federation project from conception to deployment. This guide covers the various deployment choices, the stages of deployment and potential issues you might face during deployment.

Prerequisites

This guide is not intended to be an introductory guide that explains federation concepts or what Select Federation does. This guide assumes a working knowledge and familiarity with the following:

- Federations from a business and high-level technology point of view
- Select Federation and federation terminology
- Introductory material about Select Federation

Select Federation Overview

Select Federation offers a new solution to handling the single sign-on authentication problem through a secure exchange of identity information among cooperating organizations. Whether the sign-on occurs within one company or between multiple companies using open standards, Select Federation can help companies achieve cross-domain Single Sign-On logins quickly and easily.

Typically, a user has a web account that is used regularly such as a corporate account. In addition to this account, the user may also have other independent accounts at one or more web sites that are used less frequently. After these accounts are federated, the user can access all federated web sites through the user's most frequently used account without having to log on each time.

Built on the latest federated identity standards, Select Federation does not require any radical changes to the existing technology infrastructure. It provides a de-centralized approach to cross-domain single sign-on, provisioning and privilege management across identity domains.

Select Federation offers easy integration with existing systems for (local) identity management such as access control systems, provisioning systems and Windows solutions.

For more complete information about Select Federation's features and how they work see the "Introduction" chapter in the *HP Select Federation Configuration and Administration Guide*.

2 Planning the Deployment

A typical Select Federation deployment consists of seven stages. The following sections describe each stage:

Stage 1: Understand Federated Identity Standards

Stage 2: Learn the Deployment Choices

Stage 3: Set Up Federation Architecture and Policies

Stage 4: Make a Partner Agreement for Protocol Parameters

Stage 5: Set Up an Internal Proof of Concept (PoC)

Stage 6: Set Up a Pre-production Pilot

Stage 7: Set Up a Production Environment

Once deployed, the three environments described above (PoC, Pilot and Production) need to be maintained for validating software updates, integration updates, and so on. However, maintenance is outside the scope of this document.

Stage 1: Understand Federated Identity Standards

Although there have been many choices in the recent past, federated identity standards have converged on SAML 2.0 from the OASIS SSTC as a leading choice of implementation. Another alternative is Active Directory Federation Services (ADFS), which is based on the WS-Federation protocol specification. Before deploying a federated identity system, it is a good idea to understand the basics of the protocols. See the SAML 2.0 web site for more information.

For Federated Web Services specifications, Web Services Trust Language (WS-Trust) and Liberty ID-WSF are two possible protocol choices. See the WS-Trust and Liberty web sites for more information.

Stage 2: Learn the Deployment Choices

Select Federation may be used in a variety of ways to fulfill your enterprise's need for seamless Single Sign-On and user-information sharing with trusted partner organizations. The following use-case choices determine the various possible use cases:

- **Partner Setup**: Federated identity is enabled by trust between independent partner organizations. Select Federation enables enterprises to setup trust relationships with such partner organizations and determine various communication parameters with each partner.

- **Operational Modes**: Using Select Federation, you may want to enable your users to have access to partner web sites or you may want partner employees to access your web sites or both.
- **Integration Models**: Additionally, you may already have an off-the-shelf commercial web access management system (from HP or another vendor) and may want to use Select Federation to simply integrate with the connectors that Select Federation provides out-of-box. Or you may have your own custom environment in which you require Select Federation to integrate using the rich yet easy-to-use Select Federation APIs.

Select Federation provides customers great flexibility in choosing their function, their integration environment, and the amount of customization required. You may go from being a simple identity provider with an off-the-shelf supported web-access management system backend, to being a combined IDP / SP / Federation Router with custom integration with your user database, applications and other infrastructure. Such variations in customers' existing identity infrastructure has been a key design goal for Select Federation since the beginning. Therefore, Select Federation has simple yet powerful ways of integrating in any and all such combinations.

When deploying Select Federation, you can first make a high-level determination on all the issues listed in this section before engaging in technical discussions with federation partners. This section helps you understand at a high level what choices you have and thinking about them beforehand is useful in guiding your decisions when you and your federation partners discuss various interoperability parameters.

Sometimes, a federation partner has already put in place a fairly rigid program that you need to comply with due to a business / operational mandate. In that case, you already know what your federation partner requires, so you can consider the various choices presented in this section with the partner requirements in mind.

Partner Setup

To enable a federation with a partner, Select Federation provides a powerful yet easy to use management interface for managing partners. The important considerations of managing partners are:

- Using the agreed upon protocol and its profile(s).
- Setting up a process for sharing the metadata that describes the specifics of an installation
- Specifying protocol parameters such as name policy, user consent, security profile, and so on.

Operational Modes

Identity Provider (IDP)

As an IDP (the Authority Site), Select Federation enables enterprises to locally authenticate users and convey them over one of the supported federation protocols to partner organizations. The important considerations of such a deployment typically include:

- Integrate with existing authentication infrastructure / user repository
- Determine policy regarding the user's eligibility to use / login to the partner
- Convey that authentication event to a partner using federation

- Convey appropriate information about the user to the partner
- Determine privacy policy regarding account linking of users

Service Provider (SP)

As an SP (the Application Site), Select Federation enables enterprises to seamlessly login users belonging to partner organizations to certain applications within the enterprise's domain. The important considerations of such a deployment include:

- Integrating with access management environment that is currently being used to manage access to the target applications
- Determining policy regarding to which applications external users will have access
- Determining policy regarding user's privileges within the enterprise's access management system
- Mapping the external user to an identity within the enterprise's access management system
- Acquiring and optionally storing the external user's information within the normal representation of the user within the enterprise's access management system

Federation Router

As a Federation Router, Select Federation is used to simplify trust relationships between IDPs and SPs. The Federation Router acts as an intermediary for multiple organizational entities. The Federation Router effectively acts as an SP for any IDP that has a trust relationship with it and in turn acts as an IDP for any SP that has a trust relationship with it.

The important considerations of such a deployment are mainly regarding determining policy, including:

- Which users have access to which SPs (determined based on the IDP that authenticated the user as well as additional information about the user)
- How to represent the user id when presenting the user to the SP
- How to represent the user information/attributes when presenting the user to the SP

Out-of-the-Box Access Management Connectors

Another use-case choice of deployment is how Select Federation integrates with the local environment in an installation. Select Federation supports a variety of access management connectors out-of-the box. Therefore, one common deployment choice is simply using one of the standard access management connectors (such as Select Access or COREid) to integrate with a supported local environment. The important deployment considerations in this case are the following:

- When operating as an IDP, determining which users have permission to seamlessly sign on to which of the configured SPs.
- When operating as an SP, determining how to map incoming users to either existing user ids or creating new user ids on-the-fly or some combination of the above.
- In either case, determining which users have permission to act as Select Federation administrators from the policy console of the access management connector.

Custom Integration

Sometimes, the out-of-the-box connectors may not work since your local web access management environment is not supportable by the connectors provided by Select Federation. This would happen if your web-access management vendor's product is not supported by HP or if there is something unique about your deployment of a supported WAM product that makes it impossible to use the standard connector. When integrating with a custom environment, all of the considerations of deploying a standard environment hold, and the additional considerations include:

- Determining which APIs to use for integration
- Determining how to map users in the internal security context to and from the federated context

Example of a Deployment with Custom Integration

In the case of a large enterprise running a custom-built access management Single Sign-On system, the deployment goal of the federation was to provide seamless access to employees of the enterprise to various benefits providers. Since the Access Management Single Sign-On system is custom-built, the out-of-box connectors available with Select Federation do not work. Therefore, the deployment of the IDP needed to be with a custom integration.

Following is the list of choices the customer made:

- One of the benefits provider partners was only capable of interoperating over the Liberty 1.1 protocol. Therefore the customer decided to use Liberty 1.1 for all other partners as well. Even though Select Federation can simultaneously interoperate over different protocols with different partners, the customer decided that they would like to standardize on one protocol. Since one of the partners had a constraint, they decided to standardize on the protocol supported by that partner.
- It was decided that since users had already consented to providing certain information to benefits providers, a privacy opt-in / opt-out will not be provided to users in the flow of a transaction.
- Liberty 1.1 only has the digital signature security profile, so that was chosen to be used.
- It was decided that the user-id format will be chosen on a per-partner basis, since some partners required a particular format user id that already existed in their database, while other partners were capable of mapping an opaque user id to existing benefits accounts of users.
- Customer had a custom-built web access management system. There was a choice about how to integrate with the authentication system. The customer decided to integrate at the application level using the IDPAPI of Select Federation. The other choice would have been a direct integration with the repository using the IDPPlugin API of Select Federation.

Stage 3: Set Up Federation Architecture and Policies

While much of the federation-related issues are partner dependent and require cooperation with your federation partner to set up your architecture and policies, the overall architecture and some policies can be set internally before engaging with a partner.

Operational Mode

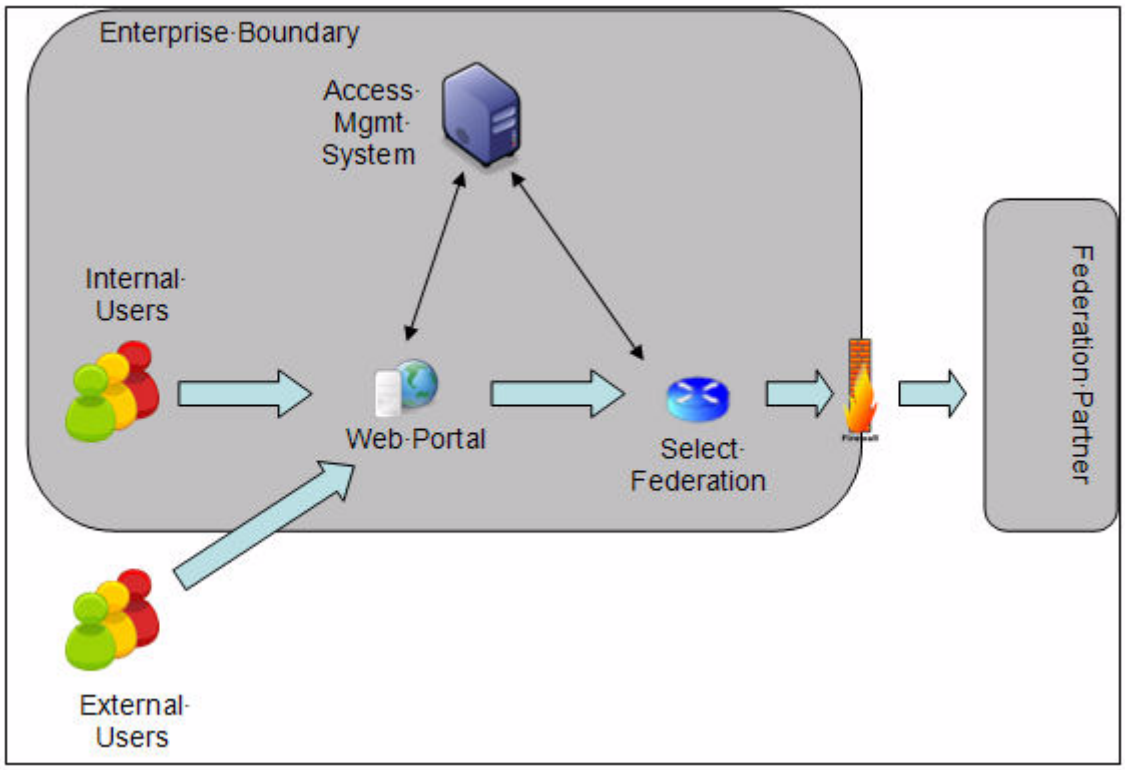
From the beginning, you may already know whether you want your users to visit partner sites seamlessly or vice versa or both. This will determine your operational mode. In some cases, you may want to phase the deployment such that you start in one direction and then implement the other. From an integration and execution point of view, it is most often easier to manage outgoing users in a federated environment than incoming users.

The next question then is how the Select Federation product will integrate with your existing infrastructure / applications in order to achieve your goals. This depends upon your operational mode.

Outbound Integration

Typical outbound integration architecture is shown in the following diagram:

Figure 1 Outbound Integration Flow



In this diagram, users (either inside the enterprise or outside the enterprise) access your web portal. The web portal has a link that normally routes the user directly to the federation partner. However, with Select Federation, you modify the link to direct the user to Select Federation and then Select Federation redirects the user to the federation partner. This allows the user to seamlessly access the federation partners' web resources without having to login again.

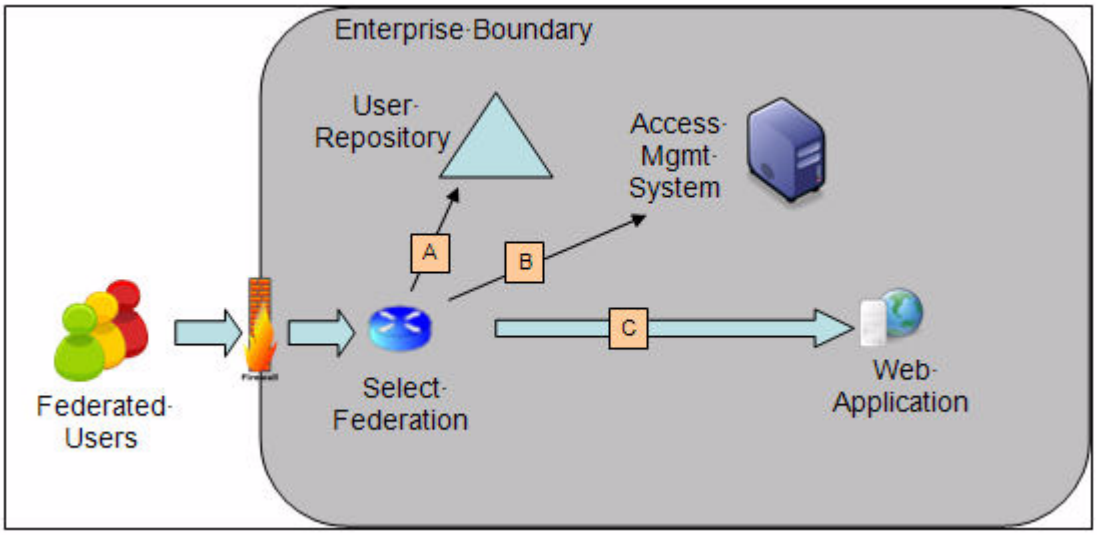
The flow in this diagram shows that users may access the web portal from inside or outside the enterprise boundary. Both the web portal and Select Federation work in cooperation with the Enterprise's identity/access management infrastructure to get the user's identity before letting the users through to the federation partner as an authenticated user.

The integration between Select Federation and the access management system may be custom or may be through one of the standard connectors available with Select Federation.

Inbound Integration

A typical flow for inbound integration is described in the following diagram:

Figure 2 Inbound Integration Flow



In this diagram, the federated users from the partner enterprise first arrive at Select Federation. The users are mapped into the local user repository (A), Select Federation obtains a “session” within the local Access Management System for them (B), and then the user is redirected to the application.

Using the above diagrams as a reference, you can come up with a high-level integration architecture for your scenario.

User Consent

If you are an Identity Provider (IDP), then you need to determine whether you want your users to consent to a federation or not. Select Federation provides a unique Privacy Manager to manage user consent for Single Sign-On as well as for attribute exchange. Depending upon the kind of information you want to exchange with your federation partner, you may consider enabling user consent so that the user can choose to not disclose such information.

You can turn on user consent in the Select Federation Administration Console, **Application Federation Policy** tab. For detailed instructions see the “Configuring the Application Federation Policy” section in the *HP Select Federation Configuration and Administration Guide*.

If you have user consent turned on, you need to design the system so that it can still function correctly if the user chooses to decline all information on which the user is allowed to give consent.

User Mapping

If you are a Service Provider, an important consideration is how you will handle users coming in to your domain. Much of this depends upon your identity environment and applications that you intend to federation enable. In some cases, it is acceptable to map a certain class of federated users to a single user entry within the local repository, whereas in other cases, each user must have a local repository copy. In the former case, the user mapping does not create any users on-the-fly, whereas in the latter case, the user entries are dynamically created. Therefore in case user entries are being dynamically created, they need to be managed manually or purged after use. You may determine what is most appropriate for your environment, but Select Federation does provide the ability to purge such users from the local directory after the session has been terminated.

Stage 4: Make a Partner Agreement for Protocol Parameters

Partners in a federation need to have a high-level business agreement regarding the conveyance of user information from the identity provider (IDP) to the service provider (SP). Depending upon the existing relationship of the partner companies, these agreements may be very simple addendums to existing partnership agreements or somewhat detailed new agreements regarding the online exchange of user information, its authenticity, security and use.

This section does not cover the logistical aspect of how to exchange operational information such as installation metadata with your partner. Such information is covered in the pre-production section of this document.

At a technical level, you will need to agree with your partners on the following choices:

- Protocol Selection
- Protocol Bindings
- User Ids and Pseudonyms
- User Attribute Sharing
- Other Protocol Security Considerations

Protocol Selection

For most new deployments, HP recommends using SAML 2.0. Some partners may be better prepared for Microsoft ADFS instead of SAML 2.0. In rare cases, you may run into partners who are only set up for older versions of SAML or Liberty. Select Federation supports all these protocols simultaneously, so you may choose to support. However, since each protocol has different properties to be managed, you may end up spending about 10% - 20% additional effort in deploying each partner who is using a different protocol. A best practice may be to recommend one protocol (such as. SAML 2.0), but be prepared to interoperate with partners that cannot support the recommended protocol.

Protocol Bindings

Federation protocols such as SAML and Liberty specify message formats and also **bindings**, which are possible ways in which the messages can be conveyed in the context of a browser-based user transaction between an IDP and an SP. For example, in SAML and Liberty, there is a **POST binding**, which specifies that the protocol message is to be delivered to an SP from an IDP through an auto-posted HTML form. Alternatively, the **artifact binding** specifies that the browser should be redirected from the IDP to the SP using a random string known as the "artifact" and that string should then be used by the SP over a SOAP call to retrieve the actual protocol message.

Federation protocols define several different profiles and bindings that are appropriate for conveying the protocol messages in different situations. For example, the SAML 2.0 protocol provides an *artifact* binding and a *POST* binding. In the artifact binding, when a user is authenticated at an IDP, he is redirected to the SP with an opaque identifier to the assertion called the *artifact*. The SP then requests the SAML assertion corresponding to the artifact from the IDP over a back-end SOAP channel. In contrast, in the POST binding, the SAML assertion is actually in the browser redirect from the IDP to the SP.

The advantage of the artifact binding is that it does not require the more "heavy" SAML assertion to pass through the browser. Depending upon what is included in the SAML assertion (such as user attributes), the assertion may be several kilobytes in size. Using the artifact binding also automatically protects against a "browser cache inspection" attack, where a hacker may get access to unauthorized information by inspecting the browser's cache. Using the artifact binding also does not require the SAML assertions to be signed (although it does not prevent them from being signed).

The advantage of using the POST profile is that it does not require any special firewall rules to enable SOAP access to the IDP's Select Federation instance. It is therefore easier to set up and sometimes necessary when the IDP is located inside the enterprise firewall, and opening it up to partners is not a viable option.

When using the artifact binding, the following additional security considerations arise:

- Direct access from the partner SP's Select Federation to the IDP's SOAP listener needs to be enabled. Some customers allow such access only on a per-partner basis rather than opening the SOAP listener to the open Internet.
- Security of the SOAP channel: Some customers require that mutually authenticated SSL be used for the SOAP channel between partners. Other choices for this include digitally signing the SOAP requests and responses using server-authenticated SSL instead of mutually-authenticated SSL. HP recommends using mutually-authenticated SSL for the best performance and security.

When using the POST profile, the following additional considerations arise:

- Any information in the SAML assertion being conveyed from the IDP to the SP is potentially vulnerable to the "browser cache inspection" attack. To avoid this possibility, use of pseudonyms for user ids and encrypting any user attributes being conveyed is recommended.
- Some browsers may have limitations on how much data can be passed through a browser POST. You may have to consider passing only a limited amount of user information due to this limitation.

User Ids and Pseudonyms

At a minimum, federation partners need to exchange user ids to know which user is in session. In some cases, a normalized user id that both recognize as the same user is required (in the case of the benefits provider example, the social security number). However, you can determine whether the partner needs to only know the user's valid and current affiliation with your organization rather than the exact identity of the user.

User Attribute Sharing

Conveying additional user information to the service provider is often required in a federation environment. You need to agree on a per-partner (or partner group) basis, which attributes are to be shared, what their expected values are and how they will be delivered.

Delivering attributes to an SP may be done in two ways:

- Including an attribute assertion in the SAML authentication assertion (push model)
- Providing a SAML attribute statement in response to a SOAP based SAML attribute query

The former has the advantage of minimizing the round trips between the IDP and SP but results in attributes being sent to the SP whether the SP wants it or not for that particular user. The latter has the advantage that attributes are release "on demand", but has the disadvantage of the additional network latency due to the multiple round-trips.

In most federation deployments, it is more efficient to push the attributes in the single sign-on assertion, since applications are not really designed for requesting attributes on demand, so all the attributes get fetched anyway.

Other Protocol Security Considerations

As we noted above, some of the security considerations are related to the choice of the protocol and protocol binding. In addition, there may be other security considerations that you need to agree with your partners on. These may include:

- **Digitally signing assertions:** While they may be a burden on performance, they are necessary from a non-repudiation point of view. Having the digital signature proves beyond doubt either within the flow of a transaction or later that a party in the federation network did indeed provide a certain request or response, that can't be denied later. This depends upon the trust between the federation partners and there is no recommendation that can work for all cases, except where it is required due to the protocol binding being used.
- **Attribute Encryption:** May be recommended due to a certain protocol binding being used, but may also be required depending upon how much the service provider trusts its web infrastructure. In some cases attribute encryption may be needed to pass the attributes through to the backend infrastructure without the web-infrastructure being able to decipher them.
- **Use of SSL with end-users:** This is highly recommended, but some service providers may want to avoid this for performance reasons (in very large scale deployments). Following some best practices, it may be acceptable to do this in a limited number of environments, where the value of information or service being accessed as a result of the identity security being offered is relatively low.

Stage 5: Set Up an Internal Proof of Concept (PoC)

Once you have high level agreement with initial federation partners on what needs to be done at the protocol level, you can get down to architecting a solution. This can be an iterative process, since once you determine the architecture you might find that you need to change something about the protocol level parameters that you have agreed with your partners.

The internal PoC may be used only initially, or on an ongoing basis to test any changes proposed to the production environment first on the PoC. The overall goal of the PoC is generally to prove that the federation deployment can technically meet the business requirements for federation. In addition, the PoC also has the following benefits

- Management can see federation in action and understand federation concepts by watching it in operation
- Architects and engineers can understand how the Select Federation software functions and get a test bed to try out various alternatives
- Architects and engineers can integrate Select Federation with existing identity / access infrastructure, and can see the end-to-end functioning in their lab environment.
- Perform use-case / functional and performance testing.
- Demonstrate advanced concepts such as load balancing and high-availability
- Testing any on-going modifications to your production environment in an internal setting.

Setting up the PoC may be very simple (if it is just to show what Select Federation is with a canned demonstration) to being elaborate (if you want to see failover and performance in action.)

PoC Environment

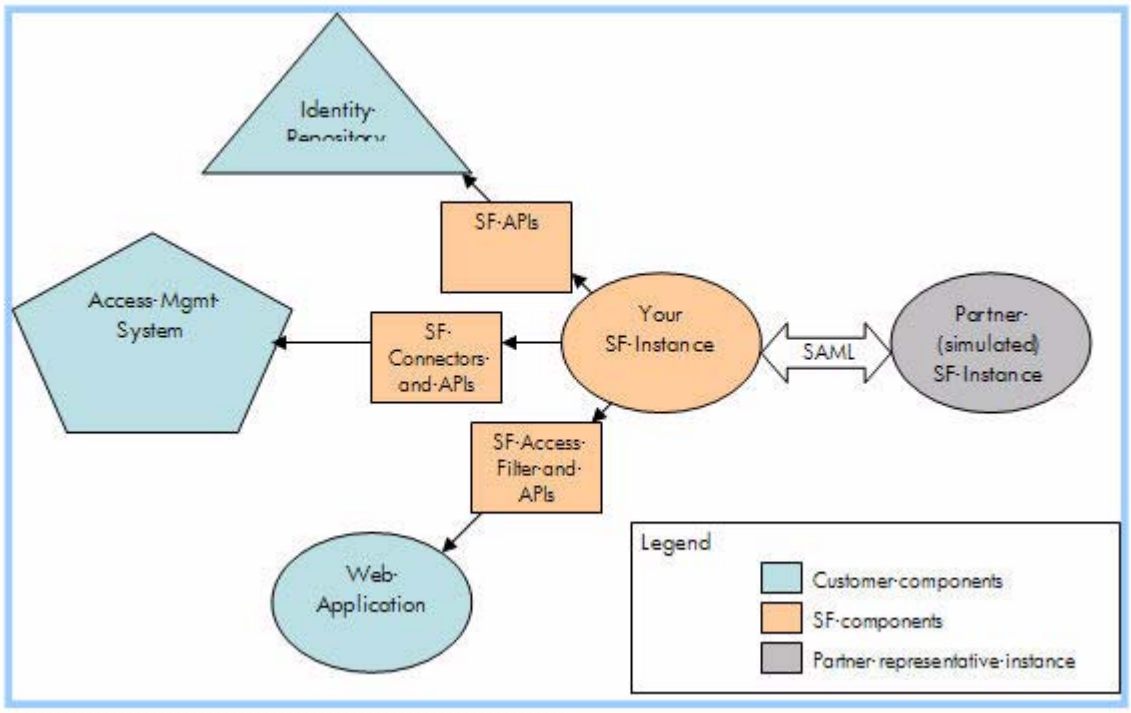
The *HP Select Federation Quick Start Guid*e refers to how you can set up an internal development environment. A similar lab environment may be used for a PoC. Based on the goals of the PoC above, you may choose to integrate the PoC with "lab" instances of your access management environment, user repository and applications.

It is recommended that the PoC cover not only the functioning of the Select Federation product, but also integration with the applications / repositories or access management products that it is going to integrate with in production, so that any integration issues are visible at the PoC stage and can be taken care of or planned around in the production environment.

It is also recommended that SSL certificates be used as they would be used in production, since some surprises may occur when you turn SSL on in production. In order to avoid that, configure SSL for the PoC as well. You may use "self-signed" certificates, since the PoC will be used only by internal browsers, in which you can add the same certificate in the trust list.

The PoC also includes a "dummy" federation endpoint that represents your federation partners. A typical PoC environment looks like the following figure:

Figure 3 PoC Logical Layout



PoC Installation Shortcuts

Use the Built-in Application Server

Select Federation offers a choice of application servers on which it can run. However, since Select Federation has a built-in application server, it is recommended that you use the built-in application server for the PoC to avoid unnecessary complications. For most PoCs, a primary goal is to validate the concept and see it in action. Only rarely does the application-server platform make a difference in the PoC.

Internal Data Repository Configuration

The Select Federation instance may be configured to use the built-in database or an external repository such as Oracle, LDAP v3 or Active Directory for storing its (internal) federation information. Sometimes, the PoC goals may include demonstrating the use of the data repository that is going to be employed in the actual production environment. However, since such use of this internal data repository is orthogonal to other integration parameters, it may be acceptable to use the built-in database for many PoCs.

SSL

If your PoC is intended to be a demonstration to management about how federation can work in your environment and is not intended to be used as a model of the production environment, you may skip SSL configuration.

If on the other hand your PoC is intended to be a “test-bed” for your production environment, then you should use SSL from the get go because adding SSL at a later time will invariably mean re-installing Select Federation. To avoid having to buy commercial certificates for the

PoC environment, you may generate self-signed certificates for the PoC environment. However, using self-signed certificates means that you have to add them to the following trusted certificate stores:

- The browsers' trust store from which you are going to access the PoC environment. This is so that when you test your PoC installation, you don't get browser warnings. This is also crucial to ensure that the redirects work as required. If you do not add the self-signed server certificate to the browser trust store, you may occasionally see blank pages in the browser.
- The Java trust stores (cacerts file). Note that each Select Federation instance has its own instance of Java, so each self-signed certificate needs to be added to each of the Java trust stores. (See the "Certificate Management" chapter in the *HP Select Federation Configuration and Administration Guide* for details.) Adding the self-signed server certificates to the Java trust stores ensures that when one instance of SF makes a web-service request to another instance of SF (typically for artifact pickup), the connection succeeds.

Not adding the self-signed certificates in the trust stores will cause SSL to not work, resulting in inexplicable behavior.

Infrastructure Integration

An important part of the PoC is to test your integration with any custom integrations/ applications that you plan to use within the production environment. Integrating with these instances also validates the connector/custom integration component of Select Federation.

Directory/Database Integration

Select Federation when functioning as an IDP relies on an external repository such as Oracle, LDAPv3 or Active Directory to fetch user attributes and optionally to authenticate users as well. Similarly, an SP can use such a repository for mapping incoming users or creating user accounts on-the-fly for federated users for use by applications. Unlike in the case of the internal data repository, it is typically very important to test this integration in a PoC as there are a number of configuration choices when connecting with the directory/database for the external repository.

Some common issues:

- When using Active Directory, often the Active Directory is running on a secure port (636) and there is no indication of it in the administration user interface. If so, you need to import the Active Directory SSL server certificate into the Java trust store of the Select Federation instance intended to connect to the Active Directory
- If the Select Federation server is on Linux and you need to connect it to an Active Directory, you will have to configure Kerberos security for the Select Federation Directory Plugin to talk to the Active Directory. This can be done by editing the `tfsconfig.properties` file and adding the line:

```
DirPlugin_ADS.ldapAuthentication=GSSAPI
```

Stage 6: Set Up a Pre-production Pilot

After you have successfully tested all important use cases in a proof-of-concept environment, you can take the next step, which is a "pre-production" pilot deployment that actually brings in users from a partner system (or conveys users to a partner system). The pre-production environment serves three purposes:

- **Initial Setup Testing**: You and your initial partner(s) can ensure that everything is working as agreed in the planning stages or changes if any are recognized and documented.
- P**artner "Onboarding" Testing**: As you add partners to your federation environment, you can leverage the Pre-production setup to ensure that your newer partners are "production ready."
- When you want to implement any updates to how the federation system works, they should first be validated on the Proof-of-Concept environment. Then to ensure that the modifications work with your existing partners, the same updates should be tried out on the pre-production environment.

Since this is the first time you will be interacting with your partners on operational logistics of federation, this is a good time to nail down some of the operational processes, such as metadata exchange, firewall configuration, federation administration, and so on.

Metadata Exchange

In federated identity environments, metadata is the union of all parameters that are required to describe a federation end-point (either IDP or SP). The individual parameters may vary based on the role of a federation end-point. For example, a SAML IDP will have a "Single Sign-On URL" as one of the metadata parameters whereas a SAML SP will have an "Assertion Consumer Service" as one of the metadata parameters. Select Federation combines all such required parameters that are allowed by standards in a file called the metadata file. In most cases, it is sufficient to exchange this file with your federation partner. However, depending upon which product your partner is running, they may or may not have a single metadata file for their end-point. Select Federation supports manual entry of such parameters through its Administration Console for this reason.

Metadata includes critical information important for the security of your federation environment, such as the certificate that your Select Federation instance uses to secure communication with partners. Although Select Federation supports signing of metadata, not all federated identity products do, so you may be exchanging metadata with your partners that your partner has no way of verifying automatically that it came from you (and vice versa). Therefore metadata should be exchanged in a reasonably secure manner. A good choice is to require exchanging metadata on a physical read-only media such as a CD in an overnight delivery service with a "signature required" to deliver the package. While this is not required for the pre-production environment, the process you set up here will help you anticipate how it should be done in production environments (potentially on a larger scale).

Metadata is very specific to a particular installation and changes if you modify certain aspects of your installation (such as getting a new signing or SSL certificate). For this reason, you need to ensure that you exchange metadata with your partners only after you are reasonably sure that your installation is not going to change.

Proxy/Firewall Configuration

Federated identity primarily relies on two communication mechanisms between partners:

- Browser access to your and your partner federation servers and web sites.
- SOAP based pickup of artifacts (in SAML and Liberty) or equivalent mechanisms in ADFS.

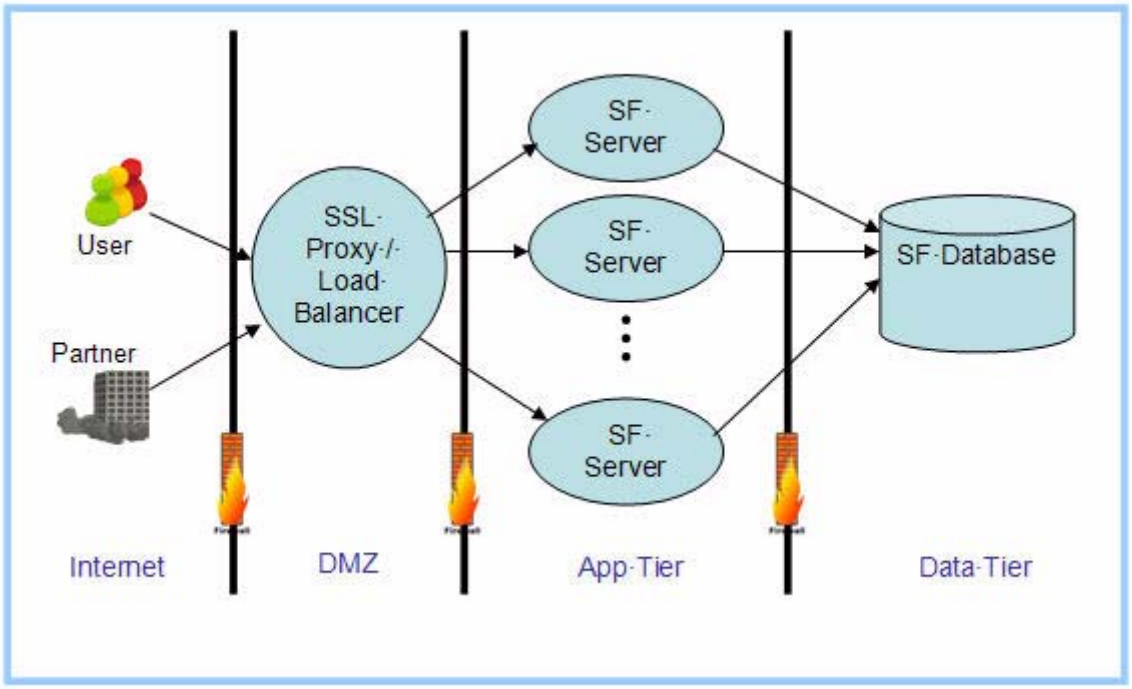
The first one presents a small challenge from a network management point of view, since users may be already accessing the web sites at partner sites even before the federation is deployed (except they would not be getting the Single Sign-On benefit). The only additional consideration is that the federation server (such as Select Federation) at the partner site needs to be accessible to your users. Similarly, the Select Federation server at your site needs to be accessible to all users who would be using the federation.

If your role is that of an IDP, users are always your existing users, so typically nothing additional is required. However, if you are acting as an SP, you need to ensure the Select Federation server is accessible to your partners' users. This might necessitate installing the Select Federation server in the Perimeter Network (DMZ). Since Select Federation does not present any UI to the user except for privacy management, it is acceptable and desirable to install Select Federation behind the Perimeter Network and installing an HTTPS proxy / load-balancer in the Perimeter Network.

The deployment architecture of a three-tier system is shown in the following figure.

While it is possible to securely deploy select federation on a single server, the unique Select Federation architecture enables it to scale as much as required.

Figure 4 Three Tier Deployment Architecture



Federation Administration

Another consideration that you can iron out in a pre-production environment is how you will administer user federations. You can construct a use-case to test the manual deletion of a user federation, should you have to do this in the real world.

To enable deleting federations without the cooperation of the user in question, the Select Federation Administration Console provides a way of manually deleting federations. When deleting a federation manually, such deletion should also be conveyed to the partner who has the other end of the federation so that the user may be “de-federated” at the partner end too. To enable this, you need to convey to your partner the “federated id” of the user you are about to delete.

Updating Partner Metadata

Another use-case that you should address in the pre-production stage is how you will update partner metadata. A partner may require to move his federation instance from one location to another or the partner may require generating a new keypair for their federation server. In any of these cases, the partner will be sending you new metadata. Select Federation administration console can update such new metadata as long as the “provider-id” of the partner does not change. If you use this way of updating partner metadata, you will be assured of retaining all the federations. If you have to delete the partner entry and create a new one, existing user federations/mappings will be removed and will not be available for future use. In such cases, it is better to dump the federation mappings to a file and then import this data back (after fixing it) to the new partner id.

Stage 7: Set Up a Production Environment

Following the process described above will ensure a smooth “go-live” experience for your installation. However, you will still have the following concerns for your production environment:

- Scalability and Reliability
- Backup and Pruning
- Disaster Recovery

Scalability and Reliability

Throughput and Latency

In browser-based federated identity systems, throughput rather than response time is the most important scalability metric today. This is because federated identity works in the context of a browser redirect (typically as a result of the user clicking on a link). In such cases, the latency of response if less than a couple of seconds is good enough as improving the latency more than that will not make a noticeable difference to the user. It is however important to ensure that the server load is maintained to such a level that latency of each transaction does not exceed the “one to two seconds” limit. If federated identity systems grow more complex with multiple intermediaries and redirects, then latency will also become an important metric.

Reliability

Reliability of a federated identity system is also extremely important since breakdown of the federated identity system will mean that users are not able to either get to the destination server at all (because the HTML links they are used to following point to the federation server) or users not being able to do single sign-on. If it is the latter (perhaps due to users having bookmarked the destination site), users will invariably flood customer service lines because they won't know or remember what password to enter at the destination site.

Scalability and Reliability Architecture

Select Federation has an architecture that allows for hot failover, potentially limitless throughput and a lot of choices for improving latency as well. The architecture described in Figure 4 on page 22 shows a model for increasing throughput as load increases. The guiding principle in Select Federation reliability and scalability design has been to leverage existing scalability technology in which network and database vendors have invested a lot of effort and not re-invent the wheel.

Web Tier

As described in Figure 4 on page 22, you can use an off-the-shelf SSL proxy / load-balancer, which sometimes also includes SSL acceleration. The load-balancer may also be clustered as specified by the load-balancer vendor. If the load-balancer is clustered, it allows for one node in the cluster to fail while retaining system availability.

Application Tier

The application tier can have multiple physical servers (or virtualized servers) for the same task, since Select Federation does not store any state in memory. This way, even if one of the servers fails, the load can be shifted automatically to the other servers doing the same task. You can optimize Select Federation performance on a limited number of hardware devices by specializing a few servers to a single task. Select Federation has independent "web-application archives" or WARs for each task, so you can choose to deploy these WARs on any overlapping combination of your application servers, as long as all these servers have access to the database.

Database Tier

From a scalability and reliability point of view, the database is perhaps the most robust part of the enterprise IT infrastructure and typically does not require special attention for the kind of load that Select Federation will impose on it. It is important to ensure though that an appropriate number of connections across all application servers are available for the Select Federation software to connect on. Since Select Federation relies on JDBC Data Sources, it is also important to use the most efficient data-source for your particular database server.

Backup and Pruning

Select Federation does not maintain any data outside the database. The database server tables created by Select Federation should be backed up according to normal database backup policies. The tables holding the federation session information need not be backed up. The names of the session tables are version specific to Select Federation, and so the product documentation for your version of Select Federation should be referenced to find the session table names.

Also, Select Federation has tables that hold audit data. These tables can be pruned to be limited to a certain size by configuring Select Federation appropriately. For audit compliance purposes, you may either use a more robust auditing system such as Select Audit or you may copy the audit table contents to a long-term backup before the table is pruned. The names of these audit tables are also version dependent.

Disaster Recovery

Select Federation can recover from emergency site closures resulting from disasters. For this to be possible, it is important to have a disaster recovery capability for the database that Select Federation is using. Once the database has been reconstituted and “taken live” at an alternative site, the same Select Federation code can be run on servers at the Disaster Recovery (DR) site. As with backup, the session tables need not be replicated at the DR site.

The consequence of starting fresh at the DR location without the session table is that some users may need to login again even if they had previously logged in to their IDP. Some users may think that they are logged out of all web sites they were logged in to, whereas in the event of such a disaster, they may not be logged out of all the web sites. Most web sites have policies that timeout idle sessions after a few hours and any compromise will require the attacker to have access to the user's browser cache. This presents an acceptable risk (in most applications) in the event of a disaster.

Glossary

Access Control

The authorization policies and conditions that regulate identity access to resources with a goal towards preventing unauthorized use or use in an unauthorized manner.

Access Management

The process of authentication and authorization.

Activation

Process of setting up mapping from a federated name identifier to a local user ID.

Active Directory Federation Services (ADFS) (WS-Federation 1.0)

A feature of Microsoft Windows 2003 Server R2, which allows a federation with Active Directory-based users, by using the WS-Federation 1.0 protocol.

Active Server Pages (ASP)

Microsoft pages, which log users in by invoking the IDP-FSS over a secure channel. See also Identity Provider Filter-Support Service (IDP-FSS).

ADFS

See Active Directory Federation Services (ADFS) (WS-Federation 1.0).

Administrator

An identity with full permission to manage Select Federation.

API

See Application Program Interface (API).

Application Helper

Select Federation component that helps you configure URLs in your application for seamless navigation to the Service Provider (SAML Consumer) sites or for authentication through the Identity Provider (SAML Producer) sites.

Application Program Interface (API)

An interface that enables programmatic access to an application.

Application Site Role

An Application Site (also called a Service Provider (SP) Site), which is a Trusted Partner site that participates in a federation to provide a service or application to common users and relies on an authority site to provide authoritative user authentication and other information. For example, in a federation of an extranet with partners' corporate portals, the site hosting the extranet is the Application Site.

Artifact Binding

Specifies that the browser should be redirected from the Authority Site (IDP) to the Application Site (SP) using a random string known as the "artifact" and that string should then be used by the SP over a SOAP call to retrieve the actual protocol message.

ASP

See Active Server Pages (ASP).

Attribute

One or more characteristics that are part of an identity profile. For each identity, an attribute has a corresponding value. For example, an attribute called "Department" may be assigned the values of, "IT", "Sales", or "Support". These attributes are interpreted and assigned appropriately to profiles in different applications (LDAP-compliant directories, databases, SAPs, and so on) based on the mapping rules defined for that application.

Authentication

The act of verifying the credentials of an identity and matching them with an identity profile. The evaluation of credentials ensures that the identity is truly who or what they claim to be.

Authority Site Role

An Authority Site (also called an Identity Provider (IDP) Site), which is a Trusted Partner site that participates in a federation to authenticate users and provide other authoritative user information to other sites. For example, in a federation of an extranet with partners' corporate portals, the portals act as the Authority Site.

Authorization

The process of defining and enforcing the entitlements of an identity. Checking whether the entitlements of an authenticated principal permit the principal to perform the requested operation. Authentication is a prerequisite for authorization. See Access Control and Authentication.

Bindings

Possible ways in which messages can be conveyed in the context of a browser-based user transaction between an Authority Site (IDP) and an Application Site (SP).

CA

Certificate Authority

CardSpace

An active client software protocol that manages the release of identity information to Service Providers (SP). Identity information is organized into "cards" on the end user's computer. Each computer contains a set of "claims" or identity attributes, such as name or email

address. Each time the user is required to authenticate to an SP, the user selects one of these cards, which determines the set of claims that will be sent.

Certificate Revocation Checking

Verifies the validity of certificates against a certification authority's published list of revoked certificates. Select Federation provides a simple means of enabling certificate revocation checking via Certificate Revocation Lists or CRLs.

Context

A Select Identity concept that defines a logical grouping of users that can access a Service.

CSR

Certificate Service Request

Delegated Administrator

An identity that has been added by the root administrator. The delegated administrator can perform all functions that the root administrator performs except admin-related functions such as add and remove admins and change admin passwords. When Select Federation is running in Standalone mode, the delegated administrator also cannot view the Admin Audit log. But when Select Federation is integrated with Select Access, then the delegated administrator can view the Admin Audit log. See Root Administrator.

DS

Discover Service

DST

(Data Services Template) DST-based services such as the Personal Profile service (ID-PP) and the Employee Profile service (ID-EP).

Edge Router

A Federation Router that is located at the edge of an enterprise where employees of that enterprise use applications offered by partners of the enterprise. Those applications request authentication of users (employees) of the Federation Router, and the Federation Router "routes" that authentication request to the appropriate departmental authority. See Federation Router.

Event

Federation activity such as **Logged In**, **Received Logout Request**, **Logged Out**, and so on. Select Federation logs server events (operational activities of enabled users) and administrator events (all the federated identity activities of each administrator).

Event Plugin Chain

A set of plugins that are called in order whenever an event occurs. A chain may contain one or more Event Plugins. See Event.

Federation

The combination of business and technology practices to enable identities to span systems, networks and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries.

Federation Router

A Select Federation installation that simplifies trust relationships between Authority Sites (IDPs) and Application Sites (SPs). The Federation Router acts as an intermediary for multiple organizational entities.

Filter-Support

A dedicated Java web application, which integrates Select Federation with the filters provided for the corresponding web servers: IIS, Apache 2.0 and Java Servlet Containers. Filter-Support also integrates Select Federation with web servers that cannot access the Select Federation databases, which are normally kept behind a firewall.

Filter-Support Service (FSS)

A servlet component that exposes Select Federation functionality to non-java applications, which can make web requests through xml messages. FSS exposes two main pieces of functionality: a) allowing trusted programs to inject a Windows-authenticated `user-id` into an IDP session, and b) allowing trusted programs to query for user attributes.

FSS

See Filter-Support Service (FSS).

GMT

See Greenwich Mean Time (GMT).

Greenwich Mean Time (GMT)

Standard time used throughout the world based on the mean solar time of the meridian of Greenwich. See Universal Coordinated Time (UTC).

Group

For Select Federation, a Group shares a common set of policies. All groups and partners within that Group inherit those policies. An administrator may override the Group setting for a particular partner within that Group.

Identity Mapping

The process of determining a local user ID against which to map an incoming federated name identifier. Two common techniques for identity mapping are either generating a random local user ID based on the federated name identifier or using any attributes available to determine a local user ID.

Identity Provider Filter-Support Service (IDP-FSS)

A servlet component of the Integrated Windows Authentication (IWA). The IDP-FSS enables a trusted program to add a Windows-authenticated user ID into an IDP session.

Identity Provider (IDP)

An Authority organization or web site that asserts the identity of users to the Service Providers or SPs in a federated network. The assertion of the user identity is done using standard protocols such as SAML and Liberty.

Identity Web Services Framework (ID-WSF)

Liberty Identity Web Services Framework security mechanism, which is a federated web service protocol. ID-WSF is used to build federated (identity-based) web services.

IDP

See Identity Provider (IDP).

IDP-FSS

See Identity Provider Filter-Support Service (IDP-FSS).

ID-WSF

See Identity Web Services Framework (ID-WSF).

IE

Internet Explorer

IIS

See Internet Information Server (IIS).

Impersonation Token

Any token that allows actions to be carried out on the user's behalf. For example, in Windows, tokens issued through Kerberos are often used for impersonating users. Various technologies running on Windows have APIs defined that take an impersonation token and apply them to threads and/or processes that can then leverage them for whatever actions they need to perform on behalf of the users.

Inbound Windows Integration (IWI)

Inbound-integration that seamlessly integrates federated users at a Select Federation Application (SP) site to applications hosted on the Windows environment.

Integrated Windows Authentication (IWA)

Outbound integration that allows Select Federation to leverage a user's Windows logon credentials to seamlessly authenticate the user and transfer the user to a Trusted Federation Partner site.

Internet Information Server (IIS)

The web server that is bundled with the Windows 2003 Server.

IWA

See Integrated Windows Authentication (IWA).

IWI

See Inbound Windows Integration (IWI).

JAVA

Object-oriented programming language.

JVM

Java Virtual Machine. A platform independent execution environment that converts Java bytecore into machine language then executes it.

Keystore

A database of keys. The private keys are associated with a certificate chain, which authenticates the corresponding public key. The keystore also contains certificates from trusted entities. By generating the keystore, you add another layer of security to the data that is exchanged in the Select Federation system.

LDAP

See Lightweight Directory Access Protocol (LDAP).

LECP

Liberty Enabled Client/Proxy Service.

Liberty Identity-based Web Services Framework (ID-WSF)

A protocol that provides standards for discovering and invoking identity-based web services.

Liberty Identity Federation Framework (ID-FF)

An open standard federation standard protocol that provides basic single sign-on capabilities.

Lightweight Directory Access Protocol (LDAP)

A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network identity can access any resource without knowing where or how it is physically connected.

Metadata

Online exact description of a Trusted Partner site in a federation. The metadata describes the various URLs at which its site services (such as Single Sign-On, Single Logout) are available. It also describes the public key certificates so that sites receiving messages from these Trusted Partner sites can confirm that the messages are signed correctly and have not been tampered with. See Single Sign-On (SSO) and Single Logout (SLO).

Microsoft Management Console (MMC)

MMC is used to set up server authentication and to import the `pkcs` / `pfx` format file into your local store on the IIS machine.

MMC

See Microsoft Management Console (MMC).

NTLM (NT LAN Manager)

Default network authentication protocol for Windows NT 4.0.

OCSP

See Online Certificate Status Protocol (OCSP).

Online Certificate Status Protocol (OCSP)

OCSP support exists in JDK 1.5. OCSP support is available for the Built-in application server (Tomcat 5.5.23) and WebLogic 8.1 and 9.1.

Partner

For Select Federation, the main entity in a federation trust relationship. A partner is described in terms of its protocol metadata, various descriptive attributes, and policy information. Select Federation allows partners to be grouped together in “Groups.”

Passive URLs

Passive URLs are for resources where users’ personalized content is not critical for the application. Users are allowed to access these URLs even though they cannot be authenticated without being prompted. However, if the user is already logged in at the IDP, has a federation session with Select Federation, or can be authenticated without being prompted, the user’s identity and attribute information is presented in the federation session to the application.

PDC

Primary Domain Controller

Plugin

Compiled code that can interact with the core product to provide additional functionality, without replacing parts of the core product. In the context of Select Federation, the “compiled code” can be thought of as Java compiled code that is packaged in JARs and the “core product” can be thought of as any Select Federation install.

POST Binding

Specifies that the protocol message is to be delivered to an SP from an IDP through an auto-posted HTML form.

Presence Service

A service that informs the WSC if a user is online, available, and so on. See Web Service Consumer (WSC).

Privacy Manager

End-user visible component of Select Federation. Its visibility allows extensive customizing.

Protected URLs

Protected URLs require users to be authenticated to allow access to these URLs. If a user is not authenticated, the filter redirects the user to Select Federation for authentication. The Select Federation installation may authenticate the user locally or initiate federated login at another Authority (IDP).

Protocol

A set of rules that controls or enables communication between two endpoints. In the context of Select Federation, an endpoint is software that is capable of using any one of the many protocols that Select Federation supports.

Root Administrator

The “super user” administrator who has complete entitlement to all functionality in the Select Federation Administration Console. The root administrator’s login is always **`admin`**. Only the root administrator can add and remove delegated administrators and change administrators’ passwords.

SAML

Security Assertion Markup Language open standard federation protocol. Identity federation standard that was created by the OASIS Security Services Technical Committee (SSTC).

Secure Sockets Layer (SSL)

A handshake protocol, which supports server and client authentication.

Service Provider (SP)

An application that allows authenticated access based on an authentication performed by an IDP using a federated identity protocol such as Liberty or SAML.

Single Logout (SLO)

Permits a user to do a global log out from all active sites.

Single Sign-On (SSO)

Session/authentication process that permits a user to enter one set of credentials (such as name/password, secureId, fingerprint, and so on) to access multiple applications. A Web SSO is a specialized SSO system for web applications.

Site Role

Type of web site in a federation. Typically, you and your Trusted Partner agree in advance on how to set up the federation. Generally, one site hosts the application, while the other provides the authentication for end users to seamlessly access the application. When you deploy Select Federation in your site, you must set the site role as one of the following: (1) an Authority Site, (2) an Application Site, (3) both an Authority and Application Site, or (4) a Federation Router. See also Service Provider (SP), Identity Provider (IDP), and Federation Router.

SOAP

Simple Object Access Protocol is a fundamental web services standard for XML-based communication between web service providers and consumers.

SP

See Service Provider (SP).

SSC

Self Signed Certificate

SSL

See Secure Sockets Layer (SSL).

SSO

See Single Sign-On (SSO).

TLS

Transport Layer Security

Universal Coordinated Time (UTC)

Standard time used throughout the world based on the mean solar time of the meridian of Greenwich. Formerly known as Greenwich Mean Time (GMT).

Unprotected URLs

Unprotected URLs allow users access to these URLs without being authenticated. Typically, special URLs such as the login URL and logout URL are unprotected URLs.

UPN

User Principal Name

UTC

See Universal Coordinated Time (UTC).

Web Service Consumer (WSC)

An application that uses web services. It may not be a web service in itself, but uses XML and typically SOAP-based communication with a web service to perform some of its functions.

Web Service Provider (WSP)

A web service application that services requests it receives based on XML and typically SOAP-based communication.

WSC

See Web Service Consumer (WSC).

WSP

See Web Service Provider (WSP).


invent


Java™
COMPATIBLE