Federated Identity in the Enterprise

Alan Abrahams

iTech Conference December 9, 2004
Agenda

- Concepts
- Overview
- Solution Models
- Planning
Concepts
Single Sign-On the Holy Grail of Authentication

- Users faced with logging into multiple applications with different username and passwords.
- Security reduced because user cannot remember the account info so they write it down.
- Difficult to integrate systems because of technology and organizational control.
- Federation is the latest attempt to overcome the barriers.
Multiple Identity Providers

Portal #1
IdP #1

Portal #2
IdP #2

Portal #3
IdP #3
Network Identity

Username
Email address
PIN
Credit Card Number
Social Security Number
Drivers License
Passport
Biometrics
Attributes:
  Employee authorization
  Roles
  Notifications
What is Federation?

- When two or more parties agree to honor the authentication mechanisms of the other parties and agree to exchange user attribute information.
  - Implies a trust relationship between the parties.
  - Federation can be implicit, this occurs when an out of band mechanism is used to federate the users identity.
  - Federation can be explicit, this occurs when the end-user initiates the federation of their identity.

- Real world examples of federation
  - US Drivers License issued by each state
  - Government issued passports
  - Bank ATM’s
Federation vs. Centralization

**Centralized Model**
- User Identity information in a single repository
- Who controls the data?
- Failure Modes
- Homogeneous Technology

**Federated Model**
- User Identity information in various locations
- No centralized control
- No single point of failure
- Heterogeneous Technology
Why use Federated Identity?

- Enterprises have multiple identity systems
  - Consolidation can be expensive
  - Organizational barriers may make consolidation difficult

- External Partner Access
  - External Partners need to access corporate Web applications
  - External partners have their own identity systems

- No Uniform Identity Management Model
  - Each enterprise establishes its own policies and procedures for managing identity.
  - Identity must be reconciled across multiple corporate and organizational boundaries.
Federated Identity Services

- **Identity Providers (IP or IdP)**
  - An entity that acts as an authentication service

- **Service Providers (SP)**
  - An entity that provides a service that consumes identity information from an IP.

- **Security Token Service (STS)**
  - A service that makes assertions about an identity based on evidence that it trusts.

- **Pseudonym Service (PS)**
  - A service that maintains alternate identity information about principals within a trust realm.
In order for a user to perform a federated authentication a trust relationship must be established:

- The service provider must trust the identity provider that is asserting the user identity.

The simplest trust relationships are for internal federation

- Two or more divisions of an enterprise may implicitly trust each other because they have common operational procedures.

With federation between two enterprises the operations procedures may be different

- An explicit trust must be established between parties so that the service provider can be assured that the identity provider is operating the identity management system within acceptable guidelines.
Business Drivers

◆ External Partner Access
  - External partner users need to authenticate to get access to e-business applications.

◆ Identity Management Cost
  - Significant costs associated with managing account information, especially passwords.
  - Federation provides the ability to outsource management overhead.

◆ Improved End-User Experience
  - Seamless transfer between services without the end-user having to log-in with multiple identities.
Benefits of Federated Identity

- Eliminates Synchronization
- Alleviate Centralized Management
- Scalability
- Independent Identity Management
OASIS Security Assertion Markup Language (SAML)
- Allows authentication, attribute and authorization information to be passed between parties in a standardized manner. Primarily used in Web based authentication.

Liberty Alliance Federated Identity Standards
- Extends SAML to provide a formal mechanism for federation across multiple web sites.

WS-Security & WS-Federation
- Provides a standard mechanism for encoding security tokens into a SOAP header and federating identity information between Web services.
Identity Mapping
- Can map identities across sites (must be done by specialized code)

Multi-Vendor Single Sign-On
- Allows single sign-on across portals by passing assertions

Attribute Passing
- By passing attribute information remote party can make an authorization decision
Inter-Site Transfer (SAML)

1. UA (browser) accesses a link on the web server.
2. UA is redirected to the inter-site transfer service (ISX).
3. UA accesses a link on the ISX, and the ISX converts the local authentication context into a SAML token.
4. UA is redirected to the relying party URL.
5. UA Accesses the relying party URL and the SAML token is passed (either thru the front channel or 5a/5b back channel) and converted to a local token.
6. UA is redirected to the target URL on the web server.
Liberty Alliance

Liberty is the only open body working to address the technical, business, and policy challenges surrounding identity and web services

- Enables interoperability between business partners
- Future-proof: built on open protocols, driving convergence
- Market's only conformance program with over 20 certified Liberty-interoperable products
- Device and platform agnostic
- Over 150 members representing a variety of industries from all corners of the globe
- Open membership policies and opportunities
- Collaboration with other standards bodies (OASIS, etc)
- Communication with privacy advocates, governments, policy groups

Source: Liberty Alliance

© 2004 Certified Security Solutions, Inc. All rights reserved.
1. Access the service provider URL
2. Redirect UA to Identity Provider
3. Login to the Identity Provider
4. Redirect UA back to Service Provider
5. Access the target URL at the service provider.
A strategy for addressing security within a Web service environment.

- It defines a comprehensive Web service security model that supports, integrates and unifies several popular security models, mechanisms, and technologies (including both symmetric and public key technologies) in a way that enables a variety of systems to securely interoperate in a platform- and language-neutral manner.

- It also describes a set of specifications and scenarios that show how these specifications might be used together.

Source: Microsoft Corporation
Basic Security Token Service

1. Authenticate and acquire token(s) from IP/STS
2. Exchange token(s) with target realm
3. Use acquired token(s) to access resource
Federated Identity Models: Service Provider Centric

- Service Provider wants to allow other enterprises or divisions to access a service offering.
- Identity Providers authenticate the users and the identity information is passed to the service provider.
- The Identity provider can pass attribute information that allows the service provider to determine roles and policies.
Multiple Service Providers want to leverage the authentication mechanisms of a single Identity Provider.

Used when an enterprise has consolidated multiple authentication systems into a centralized identity provider.

Generally part of an overall security strategy to centralize internally before federating externally.
In cross domain each “org” can take on both the role of IP and SP.

The model can be used internally within an enterprise between organizations. This applies when it is not possible to consolidate into a single IP.

The model can be used externally between different enterprises, this allows an enterprise to be an SP to another enterprise as well as a IP to others depending on the partner relationships.
Planning
Identity Management Strategy

Identity Management Elements:

- Provisioning
- Authentication
- Authorization

Federation Impacts:

- May put constraints on the scope of provisioning systems
- Service providers may have authentication security policy requirements
- Mapping access rights effects authorization policy
Federation Agreements

- **Federation Agreements**
  - Determine the rules by which the participants will play, these are akin to the Certificate Practices Statements (CPS) that govern Certificate Authority operation.

- **A federation agreement covers (but is not limited to):**
  - Technical agreements on technology interoperation
  - Policy agreements that cover authentication requirements and access rights
  - Standards for maintaining identity information by the IP
  - Auditing requirements for traceability
  - Business liability issues that may arise
  - Privacy standards for information about users shared between parties
Business Considerations

- Will you be a service provider, identity provider or both?
- How will trust be established and maintained?
- Will federation be implicit or explicit?
- How will federation impact authorization policy?
- How will federation impact authentication policy?
Federation Protocols

- The primary model for federation today is user access to web applications, interoperability is achieved using SAML and Liberty protocols.
- Future implementations of federation may extend this to web services and make use of the WS-* specifications to manage user identity between different web service applications.

Authoritative Data store

- This allows the federation service to access attribute information that is passed in the assertion. Access to the user attribute information is generally done thru a directory service.

Security Token Conversion

- Assertions often need to be converted from external format to internal format, this is the job of the Security Token Service.
Thank you

Alan Abrahams

425.216.0726 office
508.415.5399 mobile
alan.abrahams@css-security.com
Backup
References

- **SAML:**

- **Liberty Alliance:**

- **WS-Security:**

- **WS-Federation:**