Identity Federation and SSO across Organizations

Presented at Illinois Institute of Technology
NetSecure ’11 Conference and Expo, Mar 24-25, 2011
Kiran Ramineni
Ramineni@RampInfo.com
Presentation Focus

- Touch upon background of SSO
- Federation terms
- Sample SAML documents
- Implementation choices
- Benefits
Background

- Within organization (within the domain name)
- Authentication (User Id/Password, Certificate based, Other choices)
- Authorization (Group membership or User attribute – Position in the organization)
- Accounting (Who accessed what resource)

Across platforms, webserver(s) and middle ware platforms
Typical Web-SSO within an organization
Web-SSO and Federated SSO

- SSO is within an organization domain
- Federated SSO crosses the organization domain boundaries
How does Federation simplify life?

- Look at a use case of booking a travel from Chicago to San Francisco, CA.
  - Booking an airline ticket (login # 1)
  - Continuing to book a car rental (login # 2)
  - Continuing to book a hotel (login # 3)

- By Federating (uniting) your identity with all these partners, your identity is securely transferred between these organization.
Federation Terms

- COT
- IDP
- SP
- SAML (Security Assertion Markup Language)
- Assertion
COT (Circle Of Trust)
Identity Provider (IDP)

- Provides Authentication service
- Service provider redirects the users to IDP for authentication
- Asserts the user validity (based on the authentication mechanism chosen)
- Upon successful authentication, redirects to service provider with user attributes
- Can provide authentication to multiple service providers
Service Provider (SP)

- Provides a service (access to applications)
- Refers to Identity provider for authentication
- Relies on IDP provided assertion
- May authorize access to content/applications at Service provider
- Can provide service to multiple IDPs
A Simplified use case
Federation begins with COT (Meta Data Exchange)

- SAML Meta Data exchange initiates the COT prior to Federation
- IDP provides their meta data to SP
- SP provides their meta data to IDP
- Critical information for Federation is exchanged
  - Includes identifiers
  - Certificates
  - End points for various requests
IDP Meta data sample

<EntityDescriptor entityID="https://vapp1.rampinfoes.com/opensso" xmlns="urn:....:metadata">
  <IDPSSODescriptor WantAuthnRequestsSigned="false" ...>
    <ArtifactResolutionService index="o" isDefault="true" Binding="..."
      Location="https://vapp1.../opensso/ArtifactResolver/metaAlias/idp" />
    <SingleLogoutService Binding="...HTTP-POST" Location="..." ResponseLocation="..."/>
    <ManageNameIDService Binding="...HTTP-Redirect"
      Location="https://vapp1.../opensso/IDPMniRedirect/metaAlias/idp"
      ResponseLocation="https://vapp1.../opensso/IDPMniRedirect/metaAlias/idp" />
    <ManageNameIDService Binding="...HTTP-POST" Location="...">
      <NameIDFormat>urn:....:nameid-format:persistent</NameIDFormat>
      <NameIDFormat>urn:....:nameid-format:transient</NameIDFormat>
      <NameIDFormat>urn:....:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    </ManageNameIDService>
    <SingleSignOnService Binding="...HTTP-POST" Location="https://vapp1.../opensso/SSOPOST/metaAlias/idp" />
    <SingleSignOnService Binding="...SOAP" Location="https://vapp1.../opensso/SSOSoap/metaAlias/idp" />
    <NameIDMappingService Binding="...SOAP" Location="https://vapp1.../opensso/NIMSoap/metaAlias/idp" />
    <AssertionIDRequestService Binding="...SOAP" Location="https://vapp1.../opnsso/AIDReqSoap/IDPRole/metaAlias/idp"/>
    <AssertionIDRequestService Binding="...URI" Location="https://vapp1.../opnsso/AIDReqUri/IDPRole/metaAlias/idp"/>
  </IDPSSODescriptor>
</EntityDescriptor>
<EntityDescriptor entityID="https://sp.rampinfo.com/opensso" xmlns="...metadata">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="...protocol">
    <ManageNameIDService Binding="...HTTP-Redirect" Location="http://sp..../opensso/SPMniRedirect/metaAlias/sp" ResponseLocation="http://sp..../opensso/SPMniRedirect/metaAlias/sp" />
    <ManageNameIDService Binding="...HTTP-POST" Location="http://sp..../opensso/SPMniPOST/metaAlias/sp" ResponseLocation="http://sp..../opensso/SPMniPOST/metaAlias/sp" />
    <ManageNameIDService Binding="...SOAP" Location="http://sp..../opensso/SPMniSoap/metaAlias/sp" ResponseLocation="http://sp..../opensso/SPMniSoap/metaAlias/sp" />
    <NameIDFormat>...nameid-format: transient</NameIDFormat>
  </SPSSODescriptor>
  <NameIDFormat>...SAML:1.1:nameid-format: transient</NameIDFormat>
  <NameIDFormat>...SAML:1.1:nameid-format: emailAddress</NameIDFormat>
  ...
  <NameIDFormat>...SAML:1.1:nameid-format: X509SubjectName</NameIDFormat>
  <AssertionConsumerService index="0" isDefault="true" Binding="..HTTP-Artifact" Location="http://sp..../opensso/Consumer/metaAlias/sp" />
  <AssertionConsumerService index="1" Binding="...HTTP-POST" Location="http://sp..../opensso/Consumer/metaAlias/sp" />
  <AssertionConsumerService index="2" Binding="...PAOS" Location="http://sp..../opensso/Consumer/ECP/metaAlias/sp" />
</EntityDescriptor>
SAML Framework

- XML based
- Enables business partners to exchange security information
- SOAP Protocol
  - SAML Protocol
    - Request/Response
    - Assertion
      - Authentication/Subject
      - Attributes
SAML Framework

- Mostly used SAML Profiles
  - Web Based SSO profile (Focus of this presentation)
  - Enhanced Client and Proxy Profile (ECP)
  - IDP Discovery Profile
  - Single logout
Web based SSO profiles

- Two mostly used Profiles to support Browser based SSO
  - Browser post profile (BPP)
  - Browser artifact profile (BAP)
BPP (Browser Post Profile)

- May be initiated by SP or IDP
- IDP initiated
  - Build assertion using the current session
  - Post the assertion to the browser for redirection to SP
  - SP Consumes the assertion and enforces AuthZ
- SP initiated
  - Redirect to IDP
  - IDP verifies/creates a session (after successful authN)
  - Build assertion and post to the browser for redirection to SP
  - SP Consumes the assertion and enforces AuthZ
BPP (Browser Post Profile)
BAP (Browser Artifact Profile)

- The Assertion is not directly posted to the browser
- An artifact (a tag) is exchanged via browser posts/redirects
- SP submits Artifact to IDP for resolution
- IDP dereferences the Artifact and returns Assertion to SP
BAP (Browser Artifact Profile)

Browser Artifact Profile (BAP)

User

- User attempts to access
- Authenticate to IDP
- Redirect user to SP with Artifact
- Provider Artifact to SP
- Allow access based on policy

Service Provider Application

- Authenticate to IDP
- Request Assertion using artifact
- Assertion returned

Identity Provider

- Create Assertion and Artifact
- Retrieve Assertion
Assertion Components

- Assertion
  - Subject
  - Conditions
  - AuthNstatement
  - AttributeStatement
    - Attribute<Name><Value>
sample:Assertion xmlns:saml="...:assertion" ID="s22...524" IssueInstant="2011-03-04T17:47:00Z" Version="2.0">
saml:Subject>
saml:NameID Format="...:persistent" NameQualifier="https://vapp1.../opensso" SPNameQualifier="https://sp.../opensso">nI8...Z6o</saml:NameID>
saml:SubjectConfirmation Method="...:bearer" saml:SubjectConfirmationData NotOnOrAfter="2011-3-04T17:57:00Z“ Recipient="https://sp.../opensso/Consumer/metaAlias/sp"/>
<saml:Subject>
<saml:Conditions NotBefore="2011-03-04T17:37:00Z" NotOnOrAfter="2011-03-04T17:57:00Z”>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2011-03-04T17:47:00Z" SessionIndex="s20...f01"><saml:AuthnContext>
<saml:AuthnContextClassRef>...:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement><saml:Attribute Name="emailAddress">Kiran.Ramineni@rampinfoes.com
</saml:Attribute></saml:AttributeStatement>
</saml:Assertion>
Security within Federation

- Digital signatures
- Encryption
  - Transport layer
  - AuthN requests
  - Assertion content
  - Artifact resolution
- Meta data exchange
  - Digital signature requirements
  - Encryption requirements
  - Certificates
Federation Implementation choices

- User consented
  - Protects privacy
- Bulk Federated
  - Employees to access to HR system or Health Insurance application
- Auto Federation
  - Simplify user experience
- Transient
  - Just trust any one authenticated at IDP
Shibboleth And SAML

- Shibboleth was conceived for cross domain single sign on
- SAML working group was initiated in OASIS (includes Shibboleth founders)
- Liberty Alliance ID-FF, Shibboleth and SAML 1.0 converged into SAML 2.0 standard
- Shibboleth 2.x and SAML 2.0 are interoperable
Federation Used today:

- Government
  - GSA
  - E-Auth
- Educational institutions
- Commercial
  - Telcos
  - Health Care companies
  - ESPN.COM
  - Comcast.com
  - Google Apps
  - SalesForce.com
Benefits of Federation

- Organizations
  - Easily integrate with Outsourced Applications
  - Cost savings
  - User base (Identity) protection

- Individuals (Users)
  - Limited number of login/passwords to remember
  - Federate their identity between trusted/partnering organizations
Open source Products

- **OpenAM**
  - J2ee based web SSO and Federation in one product
  - Industrial strength (supports high availability and Load balanced environments)
  - Commercially supported

- **Simple SAML**
  - PHP based
  - Third party commercial support

- **Shibboleth**
  - C++ and Java
  - Third party commercial support

- Others?
Questions?
Additional Resources & References

- http://www.oasis-open.org/
- http://Shibboleth.internet2.edu
- http://www.forgerock.com/
Thanks!

For further questions or information you can reach me at

Ramineni@Rampinfo.com or
OpenAM@RampInfo.com

(630) 653-7267 Ext 111