SAML 2.0 Refresher

Oslo, Norway
August 2008

Víctor Aké
Identity and Federation Architect
victor.ake@sun.com

http://www.projectliberty.org
SAML 2

- What is it?
- What does it do?
- How does it work?
- SAML 2 components
- Web Single Sign On
- Security considerations
- Privacy recommendations
SAML 2: What is it?

- It is a standard document format to exchange security information.
- It is also a set of protocols that solves common patterns while exchanging security information.
- It is technology neutral, interoperable, and standardized.
- The standard is maintained by the OASIS Security Services Technical Committee.

OASIS = Organization for the Advancement of Structured Information Standards
SAML2: What does it do?

- Enables Single Sign On among trusted partners that reside in different DNS domains
SAML2: What does it do?

- Enables account linking (or Federation of Identities)

Sir Nils Olav

cheapfish.no

Refer to Nils Olav as xy56Xdf12
Neither of them know the user id in the other party

softice.com

Refer to Nils Olav as 45Th7812g
Neither of them know the user id in the other party

chivalrymanuals.com

Nils

NO

NOlav
SAML2: What does it do?

- Provides Single Log Out!
SAML2: What does it do?

- Enables the sharing of attributes amongst trusted partners
SAML2: What does it do?

- Can be used to convey security information outside its “native” SAML-based protocol context, i.e. Web Services.
SAML2: What does it do?

- Can be used to convey security information outside its “native” SAML-based protocol context, i.e. Web Services
Where does it fit in the Liberty specifications

Liberty Identity Federation Framework (ID-FF) & Security Assertion Markup Language (SAML) 2.0

- Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management.

Liberty Identity Services Interface Specifications (ID-SIS)

- Enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)

- Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles.

Liberty specifications build on existing standards (SAML, SOAP, WS-Security, XML, etc.)
Elements participating

Circle of trust

Asserting party (SAML Authority, Identity Provider, SAML responder)

Relying party (Service Provider, SAML requester)
SAML 2 components

Profiles
Combinations of assertions, protocols, and bindings to support interoperability for particular use cases

Bindings
Mappings of SAML protocols onto standard messaging and communication protocols

Protocols
Request/response message pairs for obtaining assertions and doing identity management

Assertions
Authentication, attribute, and entitlement information

Authentication context
Detailed data on types and strengths of authentication

Metadata
Configuration data for assertion-exchanging parties
SAML2 Assertions

- An assertion is a declaration of fact (according to someone)
- SAML assertions contain one or more statements about a subject:
  - Authentication statement: “Joe authenticated with a password at 9:00am”
  - Attribute statement (which itself can contain multiple attributes): “Joe is a manager with a $500 spending limit”
  - Authorization decision statement (now deprecated)

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Signed (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthN with user/pswd NameID = u0123451amb</td>
<td></td>
</tr>
<tr>
<td>Attribute Statement</td>
<td>favoriteColor=white mail=<a href="mailto:baah@countme.com">baah@countme.com</a> age=2</td>
</tr>
</tbody>
</table>
SAML2: Components

- Protocols
  - Authentication Request
  - Single Logout
  - Assertion Query and Request
  - Artifact resolution
  - Name Identifier Management
  - Name Identifier Mapping

- Bindings
  - HTTP Redirect
  - HTTP POST
  - HTTP Artifact
  - Reverse SOAP (PAOS)
  - SAML URI

- Profiles
  - Web Browser SSO Profile
  - Enhanced Client Proxy (ECP)
  - Identity Provider Discovery
  - Single Logout
  - Assertion Query/Request
  - Artifact resolution
  - Name Identifier Management
  - Name Identifier mapping
**Artifacts**

- An artifact is a small, fixed-size, structured data object pointing to a typically larger, variably sized SAML protocol message
  - Designed to be embedded in URLs and conveyed in HTTP messages
  - Allows for “pulling” SAML messages rather than having to push them
- SAML defines one preferred artifact format
What's in an authentication request

- **Authentication request**
  - Request ID
  - Issuer
  - Protocol version and binding
  - Assertion Consumer endpoint
  - Requested Authentication Context
  - Name ID Policy

- **Authentication response**
  - Request ID
  - In Response To
  - Issuer
  - Status code
  - Artifact or Assertion
What's in an assertion

- **Assertion**
  - ID
  - Signature (optional)
  - Subject
    - Subject confirmation
    - Name ID
  - Conditions: Time constraint, IP address, audience, etc
  - Authentication Statement
    - Authentication Instant (time stamp)
    - Session Index
    - Authentication Context
  - Attribute Statement (optional)
    - Attribute name, value pairs
    - Name spaces
Name ID Format

- Email address
- X.509 subject name
- Windows domain qualified name
- Kerberos principal name
- Entity identifier

- Persistent identifier
- Transient identifier

These 2 provide privacy-preserving pseudonyms
This provide anonymity
Authentication contexts

- Internet Protocol
- Internet Protocol Password
- Kerberos
- Mobile One Factor Unregistered
- Mobile Two Factor Unregistered
- Mobile One Factor Contract
- Mobile Two Factor Contract
- Password
- Password Protected Transport
- Previous Session
- Public Key – X.509
- Public Key – PGP
- Public Key – SPKI
- Public Key – XML Signature
- Smartcard
- Smartcard PKI
- Software PKI
- Telephony
- Nomadic Telephony
- Personalized Telephony
- Authenticated Telephony
- Secure Remote Password
- SSL/TLS Cert-Based Client Authn
- Time Sync Token
- Unspecified
- Your own customized classes...
Metadata

- Describes the configuration of a SAML entity in a standard way
  - Service endpoint URLs
  - Key material for verifying signatures
  - Supported bindings
  - Supported Name ID formats
  - Operational role, etc
- Examples of metadata
  - Identity Provider metadata
  - Service Provider metadata
IDP Initiated Web Single Sign On
SP Initiated Web Single Sign On

Authenticate when requested

Attempt access

Access resource
SP Initiated SSO with Redirect/POST bindings

1. User or UA action
2. POST signed <Response> in HTML form
3. GET using <AuthnRequest>
4. User login
5. Signed <AuthnRequest> in HTML form
6. Supply resource
7. Access resource

Service Provider sp.example.com

Identity Provider idp.example.org

Browser
SP initiated SSO with POST/artifact bindings
Account linking

Sir Nils Olav

cheapfish.no

softice.com

chivalrymanuals.com

Nils

Refer to Nils Olav as xy56Xdf12

Neither of them know the user id in the other party

NO

Refer to Nils Olav as 45Th7812g

Neither of them know the user id in the other party

NOlav
Account linking

• Account linking is the federation of identities

• Use cases
  ➢ Federation via Out-of-Band account linking
  ➢ Federation via Persistent pseudonym identifiers
  ➢ Federation via Transient pseudonym identifiers
  ➢ Federation via Identity attributes
  ➢ Federation termination
Persistent pseudonym identifier

<table>
<thead>
<tr>
<th>Local ID</th>
<th>IdP</th>
<th>Linked ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>jdoe</td>
<td>Airline</td>
<td>61611</td>
</tr>
<tr>
<td>jdoe</td>
<td>Bank</td>
<td>71711</td>
</tr>
<tr>
<td>mlamb</td>
<td>Airline</td>
<td>81811</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linked ID</th>
<th>SP</th>
<th>Local ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>61611</td>
<td>Cars</td>
<td>john</td>
</tr>
<tr>
<td>61612</td>
<td>Hotels</td>
<td>john</td>
</tr>
<tr>
<td>61621</td>
<td>Cars</td>
<td>mary</td>
</tr>
</tbody>
</table>

Identity store

Service Provider
cars.example.co.uk

Identity Provider
airline.example.com

Browser

1. Supply resource
2. Challenge for credentials, opt-in?
3. Convey signed <Response> about 61611
4. User login as john
5. Challenge for credentials, opt-in?
6. Pass along <AuthnRequest>
7. Convey <AuthnRequest> asking for persistent pseudonym
8. Assertion Consumer Service
9. User login as jdoe
10. Pass along signed <Response>

Access check

Resource
Transient pseudonym identifier

Local ID  IdP  Linked ID
n/a  Airline  294723

Linked ID  SP  Local ID
294723  Cars  john

Cache

Identity store

Service Provider
cars.example.co.uk

Resource

Assertion Consumer Service

Identity Provider
airline.example.com

Single Sign-On Service

User login as john

Challenge for credentials

Convey signed <Response> about 294723

Pass along <AuthnRequest>

Convey <AuthnRequest> asking for transient pseudonym

Access resource

Supply resource

Pass along signed <Response>

Access check

Browser
SAML 2 attribute sharing

• SAML 2.0 allows the inclusion of user attributes as attribute statements in the assertion

• Some examples on how the attribute sharing can be used
  - Transfer of profile information to personalize services
  - Transfer of attributes to create an account at the SP
  - Authorization based on the attributes received, etc

• It is important to highlight that the user should be informed about the transfer of information and if required user consent must be explicitly obtained
Privacy in SAML 2.0

- SAML supports the use of pseudonyms between an IDP and an SP, so the real name of the user does not need to be disclosed
- Transient (or one-time) identifiers
- Authentication Contexts allow user to be authenticated to a sufficient (but not more than necessary) assurance level
Security recommendations

- Message integrity and confidentiality
  - HTTP over SSL 3.0 or TLS is recommended

- Relying party requesting assertions from asserting party
  - Bilateral authentication between parties using SSL 3.0 or TLS 1.0
  - Authentication via digital signature

- Response messages via a user's web browser
  - Digitally signed using XML signature to ensure message integrity
More info:

http://www.oasis-open.org

http://www.projectliberty.org

Thanks for your time!