



SAML AND LIBERTY FOR FEDERATING IDENTITY

Eve Maler

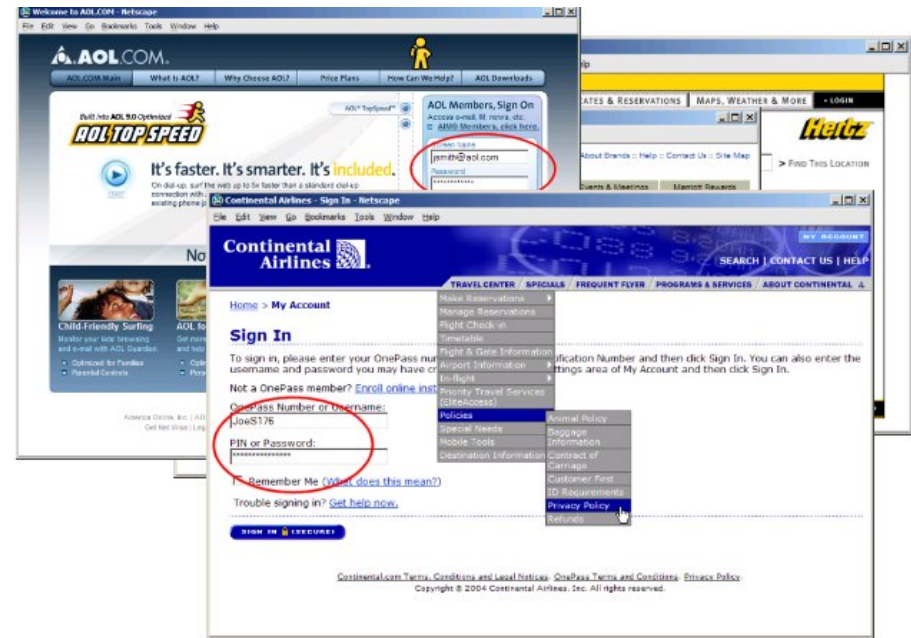
Sun Microsystems, Inc.

24 October 2005



Issues with Digital Identity Today

- Users have a proliferation of logins and passwords
- Redundantly stored attributes get out of synchronization
- Security, privacy, and cost are concerns
- When identity is not as “distributed” as the applications that need to use it, business opportunities are missed



Requirements for Federated Identity

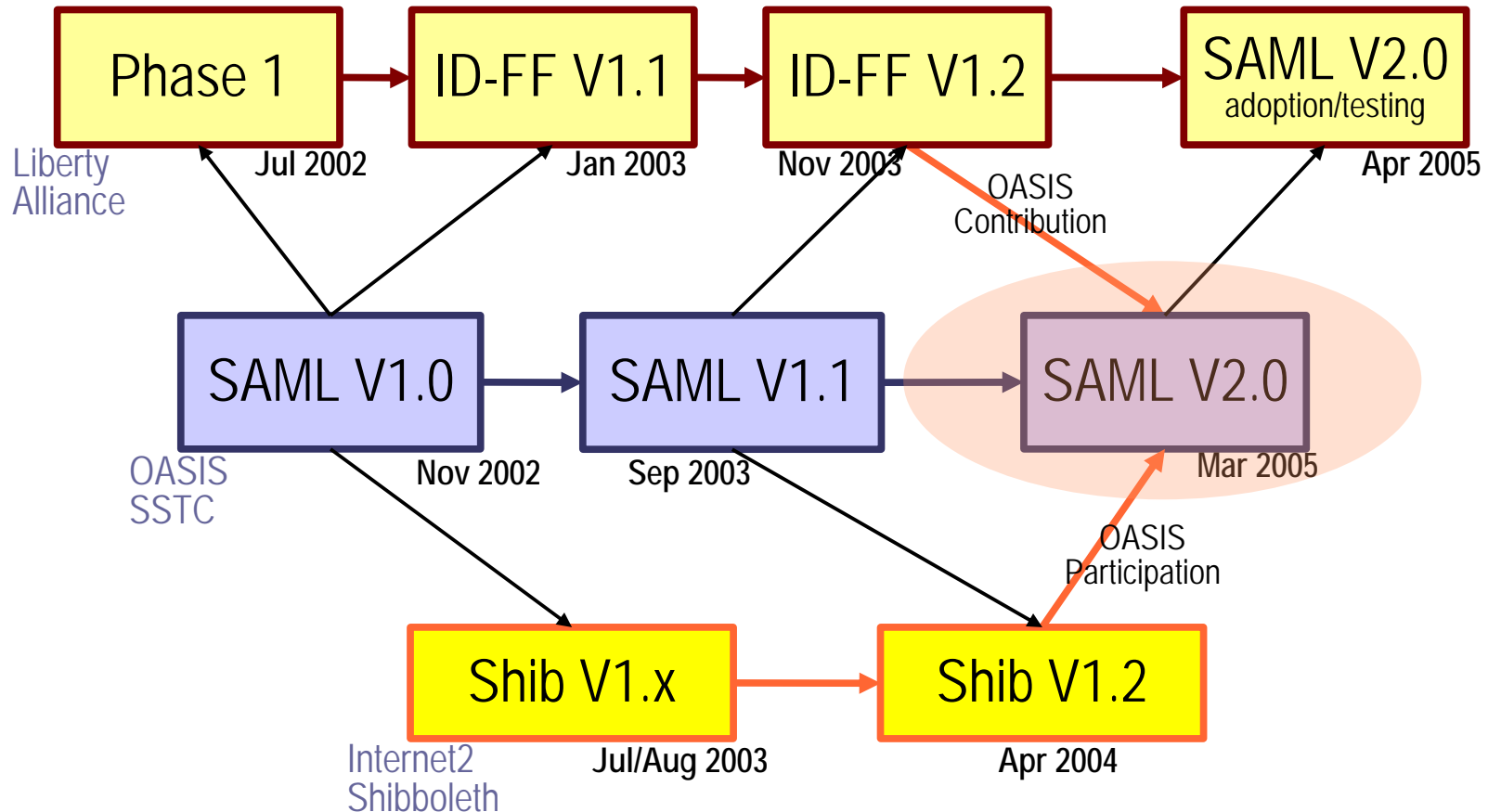
- Standard **formats** for identity information
 - > Able to represent all existing authentication and attribute technologies
- Standard, secure, privacy-enabled **protocols** for exchanging identity information between components of distributed applications
 - > Technology-neutral
 - > Well-specified and interoperable
- **A way to set up trust relationships** between applications that share identity information
 - > Within technical, business, and legal frameworks

SAML and Liberty Provide the Solution

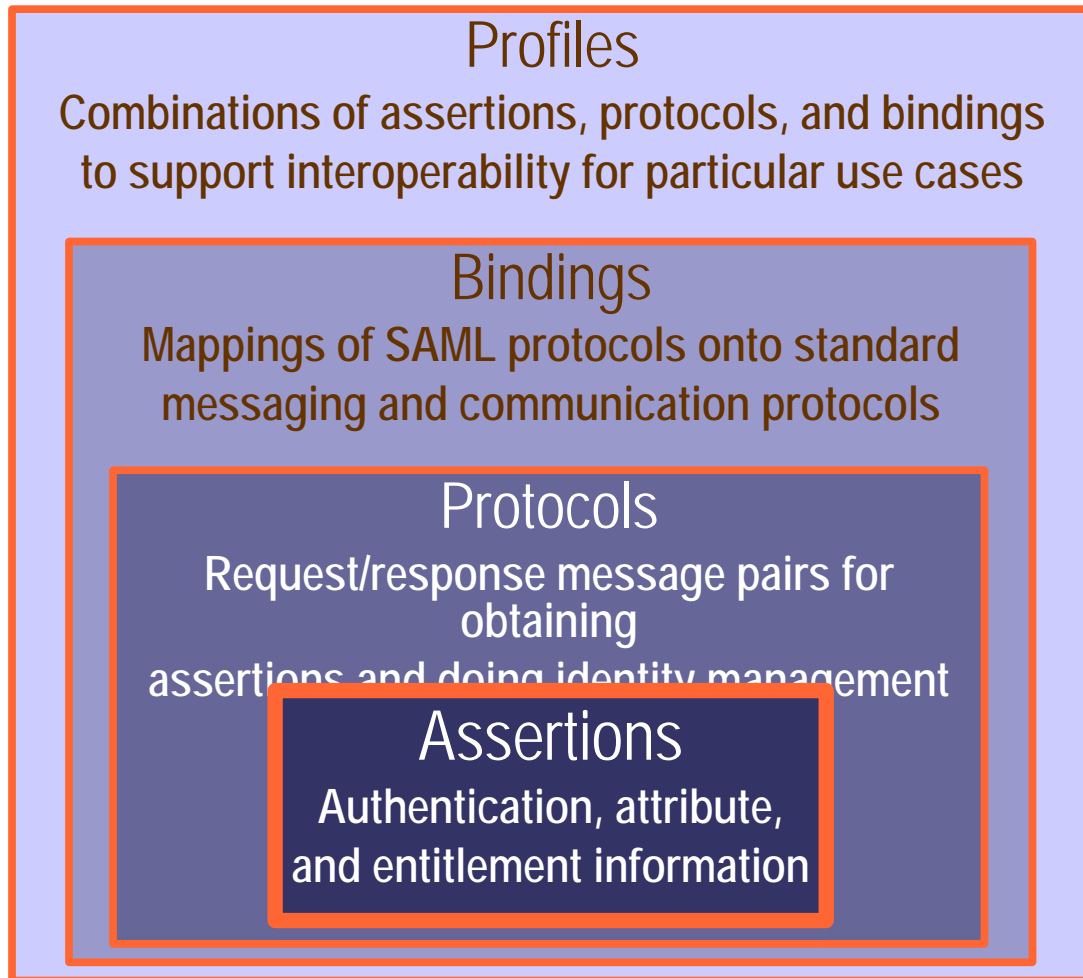
- Security Assertion Markup Language (SAML) first solved the **format** problem and provided a few **protocols for common patterns**
- Liberty developed more sophisticated **formats and protocols** based on SAML, provides **guidelines for trust relationships**, and performs **interoperability testing**
- Then SAML and (part of) Liberty converged!
 - > Learning lessons from others who have used and adapted them
 - > Particularly the Internet2 Shibboleth project

A Grand Convergence

- ID-FF = Liberty's Identity Federation Framework
 - > Liberty continues to produce other specifications: ID-WSF (Identity Web Services Framework), ID-SIS (Identity Service Interface Specifications), and more
- SSTC = Security Services Technical Committee



SAML Components



Authentication context
Detailed data on types and strengths of authentication

Metadata
Configuration data for assertion-exchanging parties

SAML Assertions

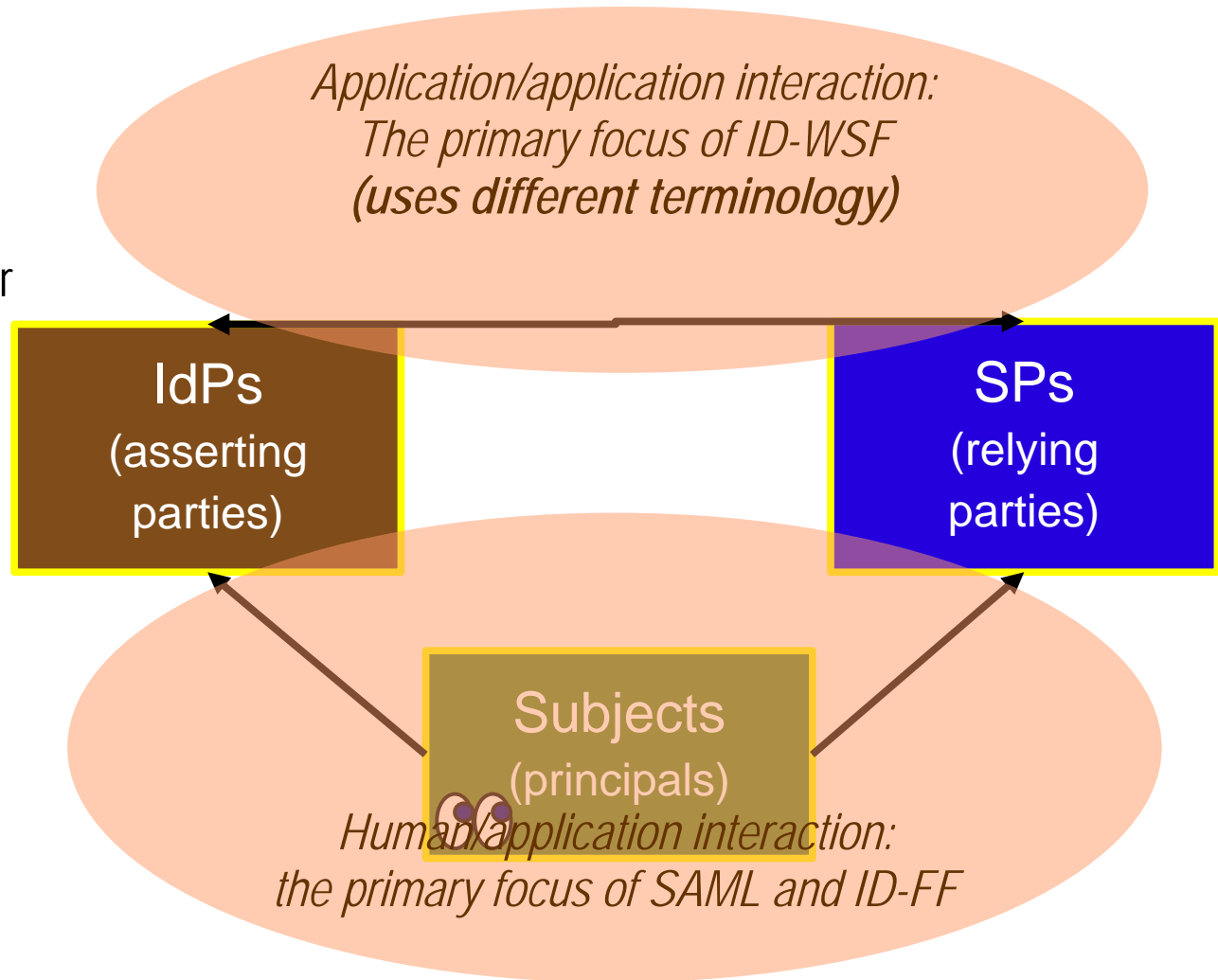
- An **assertion** is a declaration of fact (according to someone)
- SAML assertions contain one or more statements about a subject:
 - > Authentication statement: **“Joe authenticated with a password at 9:00am”**
 - > Attribute statement (which itself can contain multiple attributes): **“Joe is a manager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

SAML 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 artifact format
 - > You can create your own customized formats...

Major Entities Involved in Assertion Exchange

- **IdP** = Identity Provider (source of identity information)
- **SP** = Service Provider (consumer of identity information)
- Subjects can use clients of various types



SAML Profiles

- Web single sign-on (SSO), optionally along with attributes:
 - > Using standard browsers
 - > Using enhanced HTTP clients (such as handheld devices) that know how to interact with IdPs but are not SOAP-aware
- Identity federation – setting up agreements among providers for referring to a subject:
 - > Using a well-known name or attribute
 - > For anonymous users by means of attributes
 - > Using a privacy-preserving pseudonym
- Direct attribute retrieval:
 - > Using several common attribute/directory technologies
- Single logout – coordinated logout from multiple providers
- You can define your own customized profiles...

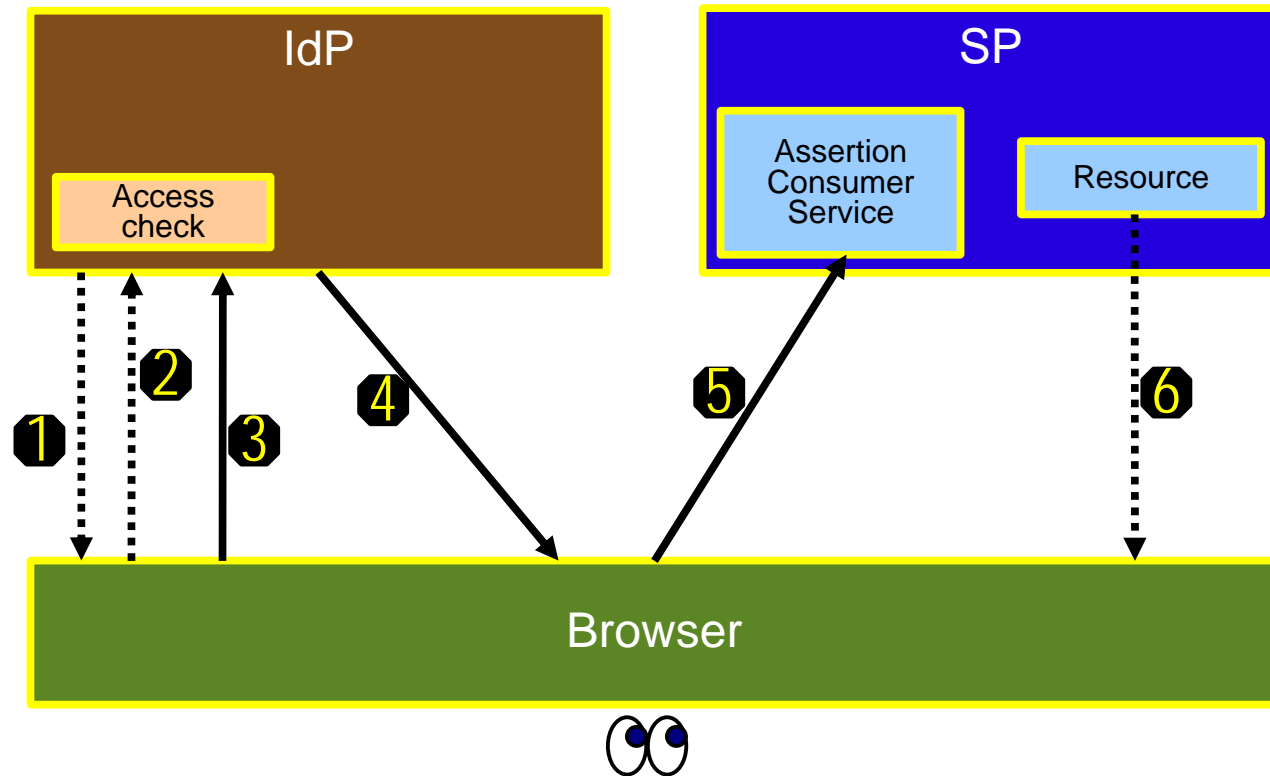
Web SSO Profile: 8 Options

- IdP-initiated:
 - > The assertion is directly “pushed” using HTTP POST
 - > An artifact is sent, then used by the SP in a query to “pull” a response message containing the assertion
 - > (2 options)
- SP-initiated:
 - > SP and IdP engage in the Authentication Request protocol
 - > SP can use HTTP POST, redirect, or artifact binding to send an authentication request
 - > IdP can use HTTP POST or artifact binding to send a response
 - > (2 x 3 = 6 options)

Web SSO Profile

IdP-Initiated – POST (“Push”) Binding

1. (Credential challenge)
2. (User login)
3. Select remote resource
4. **Put** <Response> with signed <Assertion> in HTML form
5. POST response
6. (Provide resource)

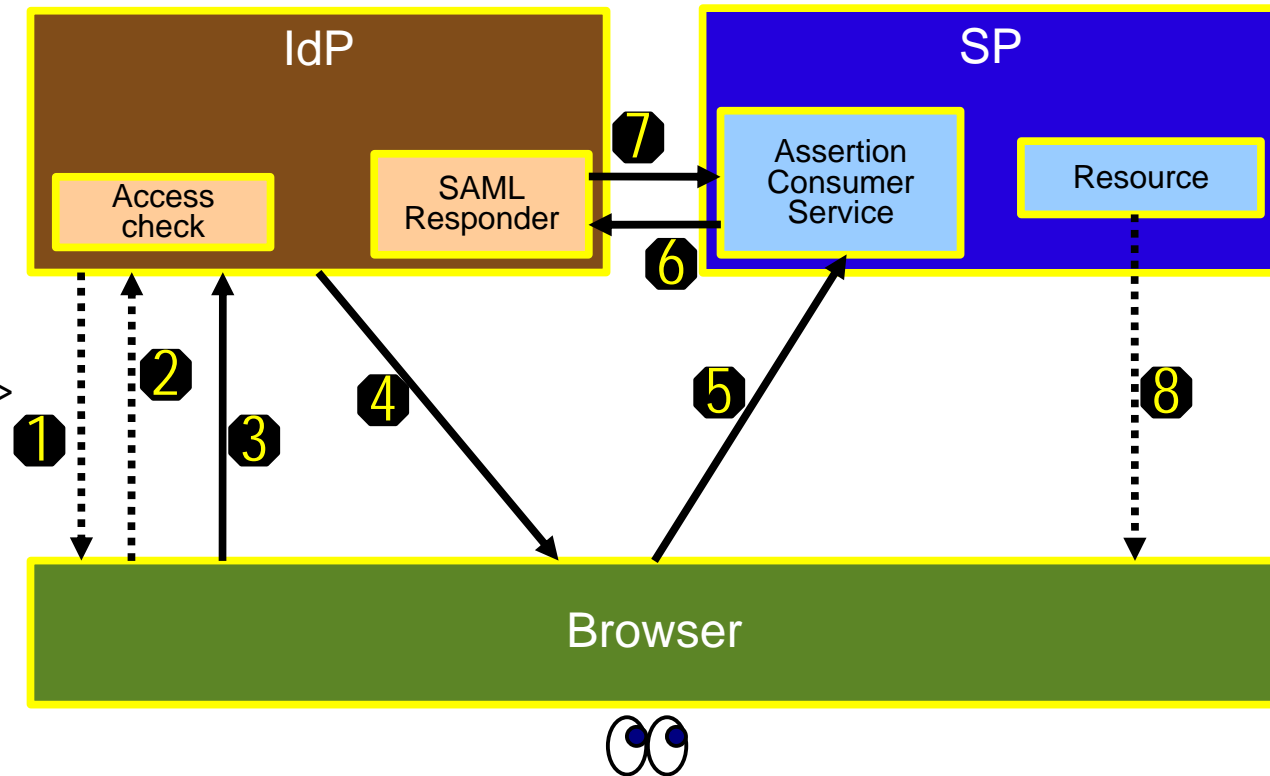


(SSO assertion could contain attribute information – e.g., “Gold status member” – also)

Web SSO Profile

IdP-Initiated – Artifact (“Pull”) Binding

1. (Credential challenge)
2. (User login)
3. Select remote resource
4. Artifact in HTML form
5. POST artifact
6. *Send* <ArtifactResolve>
7. *Send* <ArtifactResponse>
8. (Provide resource)



SAML Conformance and Operational Modes

- Profiles are the “minimum unit of interoperability”
- But **operational modes** are the “minimum unit of conformance”
- Each one requires support for a particular set of profiles
 - > IdP or IdP Lite
 - > SP or SP Lite
 - > ECP (Enhanced Client or Proxy)
 - > SAML Authentication Authority, SAML Attribute Authority, SAML Authorization Decision Authority (Policy Decision Point)
 - > SAML Requester

Example of the Common Portions of an Assertion

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Version="2.0"
  IssueInstant="2005-01-31T12:00:00Z">
  <saml:Issuer>
    www.acompany.com
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format=
        "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
        j.doe@acompany.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2005-01-31T12:00:00Z"
    NotOnOrAfter="2005-01-31T12:00:00Z">
  </saml:Conditions>
    ... statements go here ...
</saml:Assertion>
```

Example of an Authentication Statement

```
<saml:AuthnStatement
  AuthnInstant="2005-01-31T12:00:00Z"
  SessionIndex="6777527772">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
```


Authentication Context Classes

- 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...**

Example of an Attribute Statement

```
<saml:AttributeStatement>
  <saml:Attribute
    NameFormat="http://smithco.com">
    Name="PaidStatus"
    <saml:AttributeValue>
      PaidUp
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    NameFormat="http://smithco.com">
    Name="CreditLimit"
    <saml:AttributeValue xsi:type="smithco:type">
      <smithco:amount currency="USD">
        500.00
      </smithco:amount>
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Attribute Profiles

- Basic
 - > Simple string-based SAML attribute names
- X.500/LDAP
 - > Common convention for SAML attribute naming using OIDs, expressed as URNs and accompanied by usage of **xsi:type**
- UUID
 - > SAML attribute names as UUIDs, expressed as URNs
- DCE PAC
 - > DCE realm, principal, and primary group, local group, and foreign group membership information in SAML attributes
- XACML
 - > Mapping of SAML attributes to an XACML attribute representation

Guidelines and Other Assistance

- From the **OASIS SSTC**:
 - > Executive Overview, Technical Overview, presentations
 - > saml-dev@oasis-open.org discussion list
 - > <http://www.oasis-open.org/committees/security>
- From the **Liberty Alliance**:
 - > Circle of Trust Legal Framework document
 - > Implementation Guidelines
 - > Business Guidelines for Mobile Deployments
 - > Privacy and Security Best Practices
 - > And much more...
 - > <http://www.projectliberty.org>

SAML AND LIBERTY FOR FEDERATING IDENTITY

Eve Maler

eve.maler@sun.com

<http://www.xmlgrl.com/blog>

