Security Assertion Markup Language (SAML)

Vika Felmetsger

SAML as OASIS Standard

- OASIS Open Standard
- SAML V2.0 was approved in March, 2005
- Blending of two earlier efforts on portable trust:
  - S2ML
  - AuthXML
- SAML V1.0 was approved in November 2002

SAML: The Big Picture

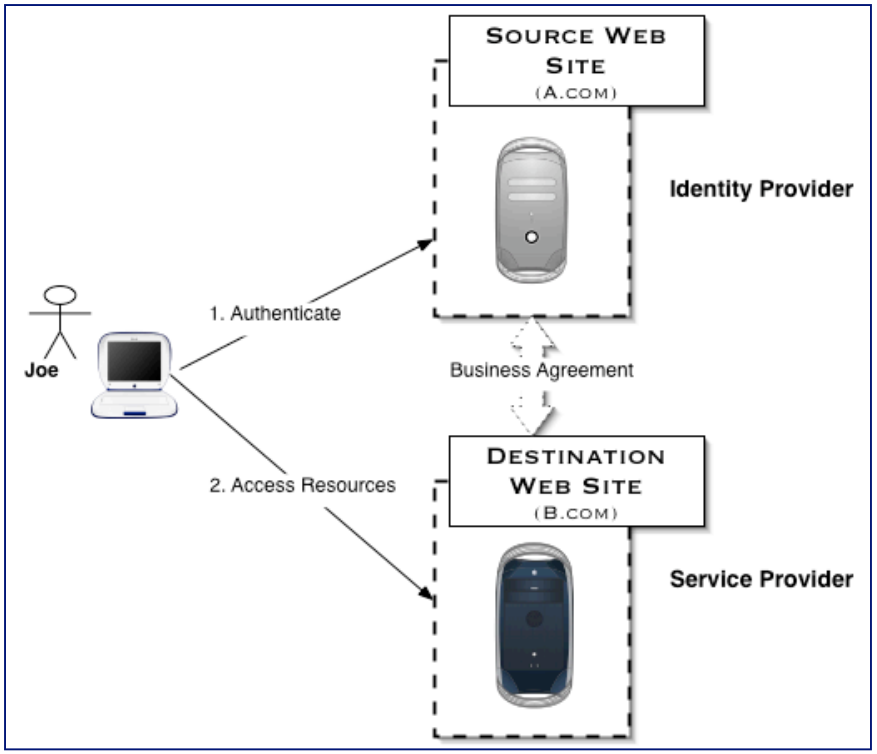
- Is another XML-based Standard
- Is a framework for exchanging security information between business partners
- Is based on the concept of Assertions (statements about a user) which can be passed around
- Provides a standard request/response protocol for exchanging XML messages

Why do we need SAML?

- "Portable Trust" - a user, whose identity is established and verified in one domain, can invoke services in another domain
  - Cross-Domain Single Sign-On (SSO)
  - Federated Identity
- Web Services - provides a means by which security assertions about messages and service requesters can be exchanged

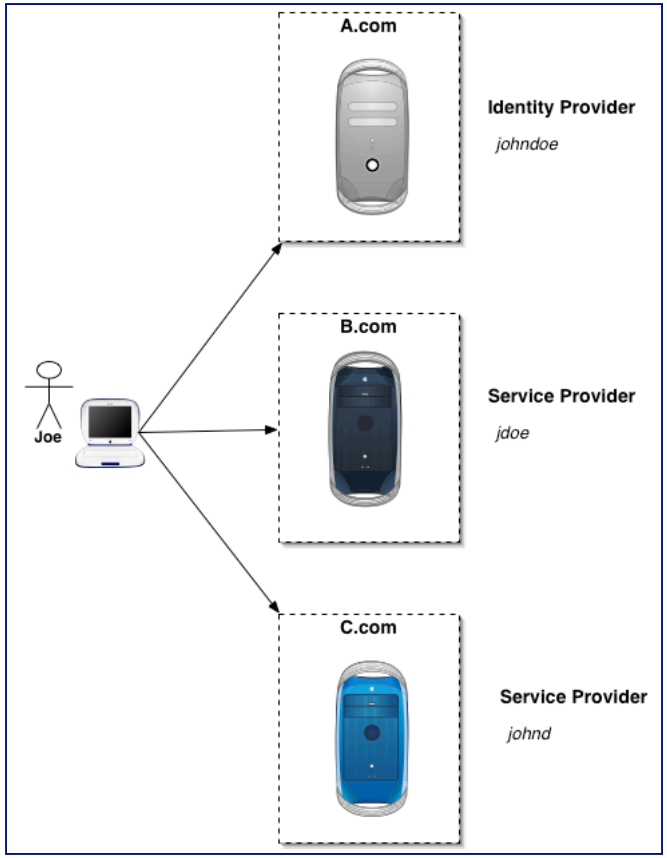
Single Sign-On

- A user authenticates to one web site (domain) and then is able to access resources at some other web sites (domains)
- A user Joe is authenticated at A.com and can access resources at both A.com and B.com



Federated Identity

- A set of service providers agrees on a way to refer to a single user even if he/she is known to each of them under a different name
- The user Joe is authenticated at A.com as *johndoe* and can access resources at both B.com (*jdoe*) and C.com (*johnd*) without being re-authenticated



SAML Assertions

- Assertion is a claim, statement, or declaration of fact made by some SAML authority
- Types of assertions:
  - Authentication - the subject was authenticated by a particular means at a particular time
  - Authorization - the subject was granted or denied access to a specified resource
  - Attributes -the subject is associated with the supplied attribute

Assertion Example

```
1 <saml:Assertion
2      Version="2.0"
3      ID="_34234se72"
4      IssueInstant="2005-04-01T16:58:33.173Z">

5   <saml:Issuer>http://authority.example.com/</saml:Issuer>
6   <ds:Signature>...</ds:Signature>
7   <saml:Subject>
8      <saml:NameID format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
9        jygH5F90l
10     </saml:NameID>
11  </saml:Subject>

12   <saml:AuthnStatement
13     AuthnInstant="2005-04-01T16:57:30.000Z">
14       <saml:AuthnContext>
15         <saml:AuthnContextClassRef>
16           urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
17         </saml:AuthnContextClassRef>
18       </saml:AuthnContext>
19   </saml:AuthnStatement>
20 </saml:Assertion>
```

Common Elements

- <Issuer> - the issuer name [Required]
- <ds:Signature> - an XML signature for integrity protection and authentication of the issuer [Optional]
- <Subject> - the subject of the statements in the assertion [Optional]
- <Conditions> - must be evaluated when using assertions [Optional]
- <Advice> - additional info that assists in processing of assertions [Optional]

Assertion Statements

- <Assertion> contains zero or more of:
  - <AuthnStatement> - an authentication statement
  - <AuthzDecisionStatement> - an authorization statement (finalized in SAML V2.0)
  - <AttributeStatement> - an attribute statement
  - <Statement> - custom statement type

Encrypted Assertions

- Intended as confidentiality protection
- Identified by <EncryptedAssertion>
- <xenc:EncryptedData> [Required] - details are defined by XML Encryption
- <xenc:EncryptedKey> [Zero or More] - decryption keys

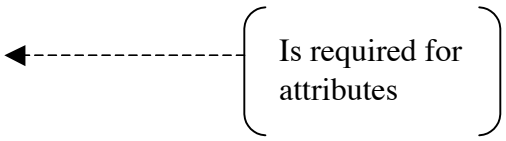
Example of Attribute Assertion

```
<saml:Assertion …>

  <saml:Issuer> … /saml:Issuer>
  <saml:Subject>…</saml:Subject>

  <saml:AttributeStatement>
   <saml:Attribute
     Name="PaidStatus">
      <saml:AttributeValue>
            Paid
      </saml:AttributeValue>
   </saml:Attribute>

  </saml:AttributeStatement>
</saml:Assertion>
```

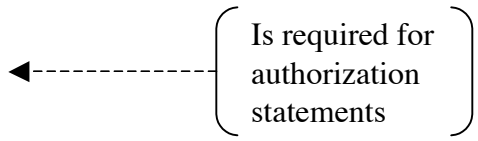


Example of Authorization Assertion

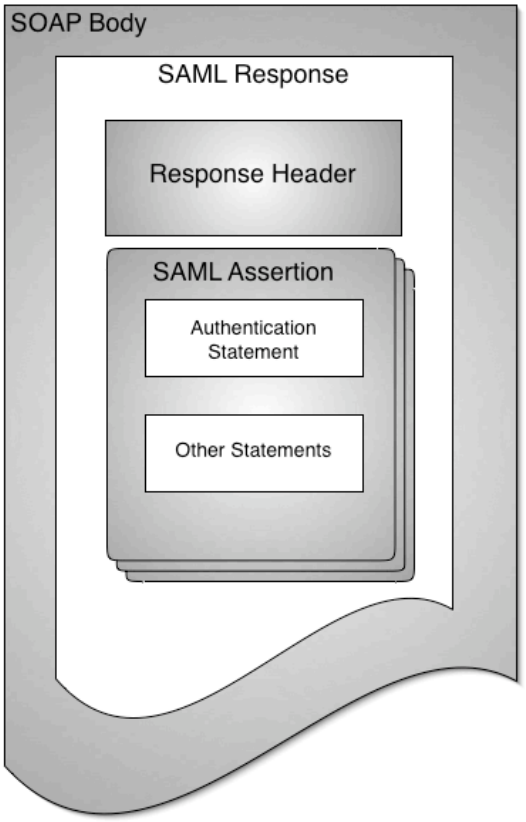
```
<saml:Assertion …>

   <saml:Issuer> … /saml:Issuer>
   <saml:Subject>…</saml:Subject>

   <saml:AuthzDecisionStatement>
     Resource="http://CarRentalInc.com/doit.cgi"
     Decision="Permit">
      <saml:Action>
            Execute
      </saml:Action>
   </saml:AuthzDecisionStatement>
</saml:Assertion>
```



Assertion Containment



SAML Protocols

- A number of request/response protocols for communicating with SAML authority
  - Retrieve existing assertions
  - Request authentication of a principal
  - Request a near-simultaneous logout
  - Request a name id to be mapped into another one
  - Etc.

Example of Request

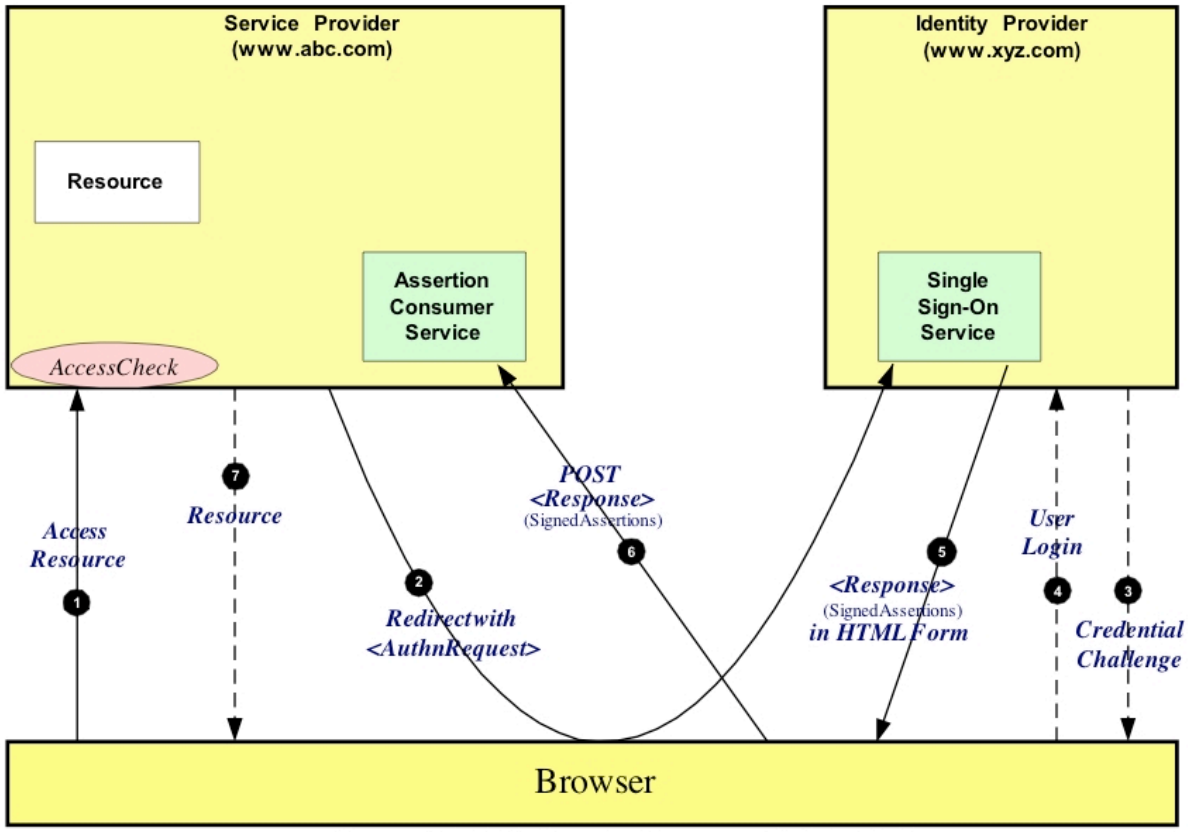
```
POST /SamlService HTTP/1.1
Host: www.example.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV=”http://schemas.xmlsoap.org/soap/envelope/”>
    <SOAP-ENV:Body>
        <samlp:AttributeQuery xmlns:samlp:=”…”
xmlns:saml=”…” xmlns:ds=”…” ID=”_6c3a4f8b9c2d” Version=”2.0”
IssueInstant=”2004-03-27T08:41:00Z”
            <ds:Signature> … </ds:Signature>
            <saml:Subject>
            …
            </saml:Subject>
        </samlp:AttributeQuery>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Example of Response

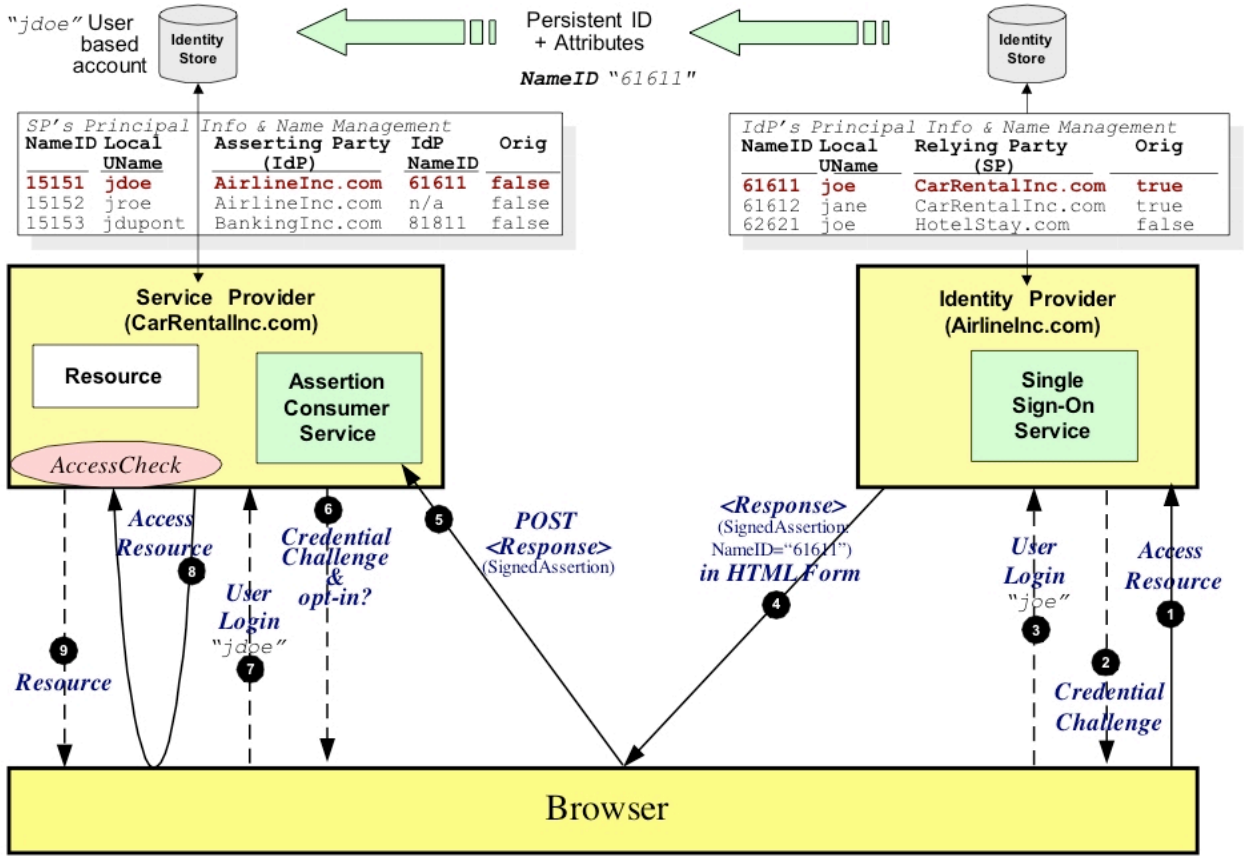
```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:Response xmlns:samlp="…" xmlns:saml="…" xmlns:ds="…"
ID="_6c3a4f8b9c2d" Version="2.0" IssueInstant="2004-03-27T08:42:00Z">
            <saml:Issuer>https://www.example.com/SAML</saml:Issuer>
            <ds:Signature> … </ds:Signature>
            <Status>
              <StatusCode Value="…"/>
            </Status>

            <saml:Assertion>
                <saml:Subject>
                …
                </saml:Subject>
                <saml:AttributeStatement>
            …
                </saml:AttributeStatement>
             </saml:Assertion>
        </samlp:Response>
    </SOAP-Env:Body>
```

SSO Profile Example



Federation Example



SAML and XACML

- XACML - an XML-based language for access control
  - XACML and SAML were designed to complement each other:
    - An XACML policy can specify what to do with SAML assertion
    - XACML-based attributes can be expressed in SAML

SAML and WS-Security

- WS-Security - a framework for securing SOAP messages
  - Different profiles for various security token formats (such as X.509 certificates and Kerberos tickets)
  - There is also a SAML token profile for SAML assertions

SAML: In Summary

- Portable Trust across domains
- Platform independent
- Standard message exchange protocol
- Easily extendable

SAML in Production

- Entegrity's AssureAccess
- Entrust's GetAccess portal
- Netegrity's AffiliateMinder
- Sucurant's RSA Cleartrust
- Sun's iPlanet Directory Server with Access Management
- Sun's ONE Network Identity
- Systinet's WASP Secure Identity
- others

References

- H. Lockhart et al, "Security Assertion Markup Language (SAML) V2.0 Technical Overview" , http://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf
- P. Madsen, "SAML 2: The Building Blocks of Federated Identity", http://www.xml.com/pub/a/2005/01/12/saml2.html
- P. Mishra et al, Security Assertion Markup Language (SAML) V2.0, http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=security
- M O'Neill et al., Web Services Security
- J. Rosenberg and D. Remy, Securing Web Services with WS-Security