SAML 2.0

Security Assertion Markup Language

Mark Allen Earnest
Lead Systems Programmer
Emerging Technologies
The Pennsylvania State University

What is SAML?

- A method of representing authentication and authorization data in XML
- Developed by OASIS, Version 2.0 was released March 2005
- Used by Shibboleth, Liberty Alliance, and Lionshare

How is SAML Used?

- WebSSO
- Attribute-Based Authorization
- Securing Web Services

SAML Components I

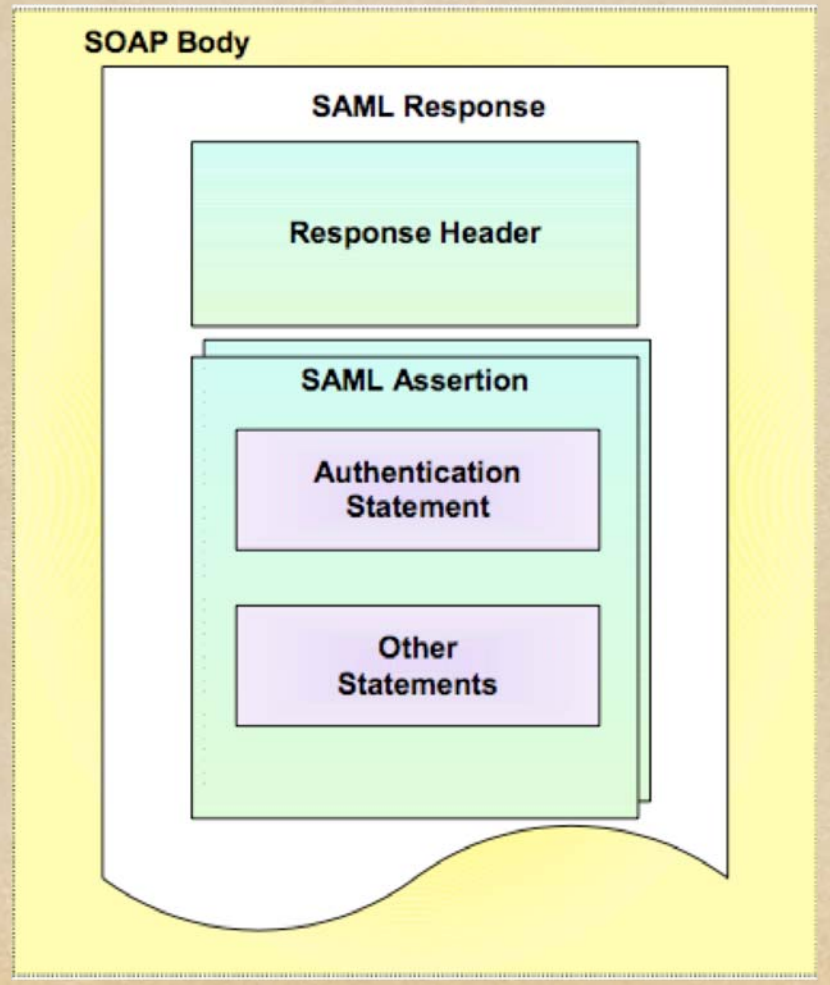
- Assertions
  - Authentication
  - Attribute
  - Authorization Decision

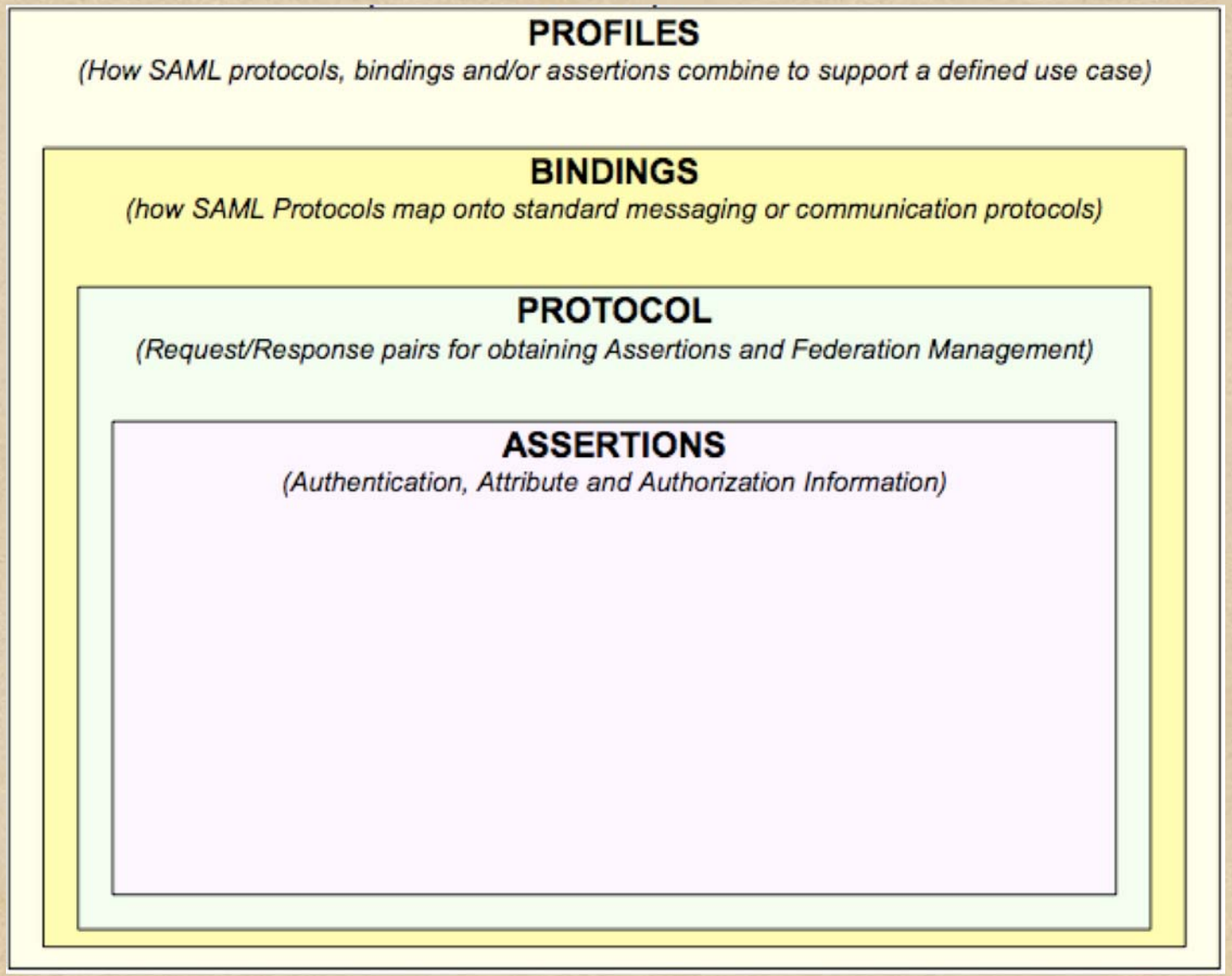
SAML Components II

- Protocols
  - Request assertions from SAML Authority
  - Request an identifier be registered
  - Request an identifier be terminated
  - Request a simulations logout of all sessions

SAML Components III

- Bindings
  - SOAP
  - HTTP
- Profiles




PROFILES
(How SAML protocols, bindings and/or assertions combine to support a defined use case)
BINDINGS
(how SAML Protocols map onto standard messaging or communication protocols)
PROTOCOL
(Request/Response pairs for obtaining Assertions and Federation Management)
ASSERTIONS
(Authentication, Attribute and Authorization Information)

Sample SAML Assertion

```
<Assertion AssertionID="fcd0b7ff-8296-4e5b-91e5-5bc042100323" IssueInstant="2003-01-16T17:05:58Z"
Issuer="psu.edu" MajorVersion="1" MinorVersion="0">
 <Conditions NotBefore="2003-01-16T17:05:58Z" NotOnOrAfter="2003-01-16T17:05:58Z">
  <AudienceRestrictionCondition>
   <Audience>http://middleware.internet2.edu/shibboleth/clubs/clubshib/2002/05/</Audience>
  </AudienceRestrictionCondition>
 </Conditions>
 <AttributeStatement>
 <Subject>
  <NameIdentifier NameQualifier="psu.edu">b8d3d86c-03e3-4582-b6c8-8340cc9fd0f1</NameIdentifier>
   <SubjectConfirmation>
    <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:Bearer
    </ConfirmationMethod>
   </SubjectConfirmation>
  </Subject>
  <Attribute AttributeName="urn:mace:eduPerson:1.0:eduPersonPrincipalName"
AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <AttributeValue xsi:type="typens:eduPersonPrincipalNameType">mxe20</AttributeValue>
 </Attribute>
 </AttributeStatement>
</Assertion>
```

New in SAML 2.0

- Pseudo-anonymous Handle
- IdP Discovery
- Encryption for individual attributes, name identifiers, and entire assertions
- Attribute Profiles
- Session Management
- Privacy Mechanisms

OpenSAML

- Set of Java and C++ classes to build, transport, and parse SAML Assertions
- Implements HTTP-POST & SOAP SAML Profiles
- Developed by Internet2
- Open Source

Vendor Support

- IBM WebSphere announced support for SAML in November 2003
- Oracle, Computer Associates, and RSA's identity management software already supports SAML 2.0
- More software integration planned

WS-Fed

- Introduced by Microsoft & IBM as an alternative to SAML
  - Both previously were involved in SAML working group
- Interop being worked on, nobody knows for sure at this point how much interop.

SAML @ PSU

- Shibboleth
  - Webassign
  - Napster
- Lionshare

Questions?

- Thank you
- mxe20@psu.edu