Internet2 Middleware Initiative

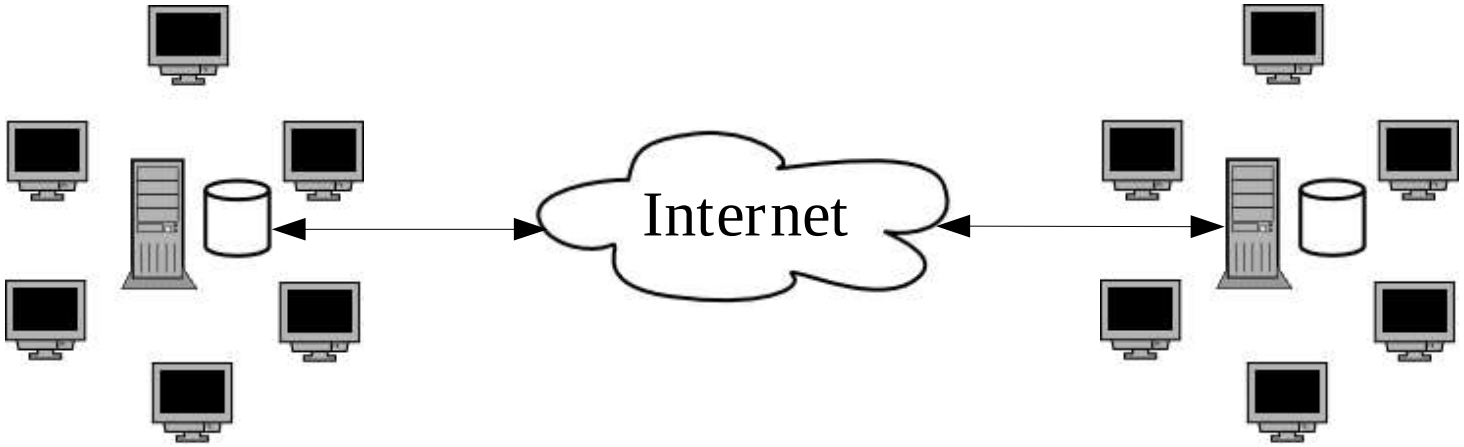
Inter-realm authentication and authorization using eduPerson, SAML, OpenSAML, and Shibboleth

Mark Earnest
Lead Systems Programmer
Academic Services & Emerging Technologies
Pennsylvania State University
mxe20@psu.edu

PENNSTATE

The Problem

- Universities have different network authentication systems.
- Universities want to be able to share resources with other universities.
- Universities want to retain authorization control over what they share.
- There is no common way to describe user attributes.
- Universities are very protective of their authentication databases.



University A
Kerberos

University B
PKI

PENNSTATE

Bad Solutions

- Filter by IP address
  - Broadband
- Maintain accounts for inter-realm users
  - Annoying to end user (multiple accounts)
  - Administrative nightmare
  - Poor scaling
- Synchronize Authentication Databases
  - Administrative nightmare
  - Security nightmare
- No Security
  - Not an option for licensed resources
  - Even without security, identity is still needed
- Microsoft Passport

PENNSTATE

Good Solutions

- Develop an inter-realm schema to identify user attributes
- Agree to trust each other's authentication system and user attributes
- Develop a common security protocol that can be used by universities to "assert" identity and attribute information to each other
- Use Open Source and open standards every step of the way :)

PENNSTATE

eduPerson

- An LDAP object class to describe individuals in higher education
- Common attribute names and allowed values agreed upon
  - eduPersonPrincipalName
  - eduPersonAffiliation
  - eduPersonEntitlement
  - eduPersonOrgDN
  - eduPersonNickname
  - and others....
- Co-developed by Educause/Internet2
- http://www.educause.edu/eduperson/

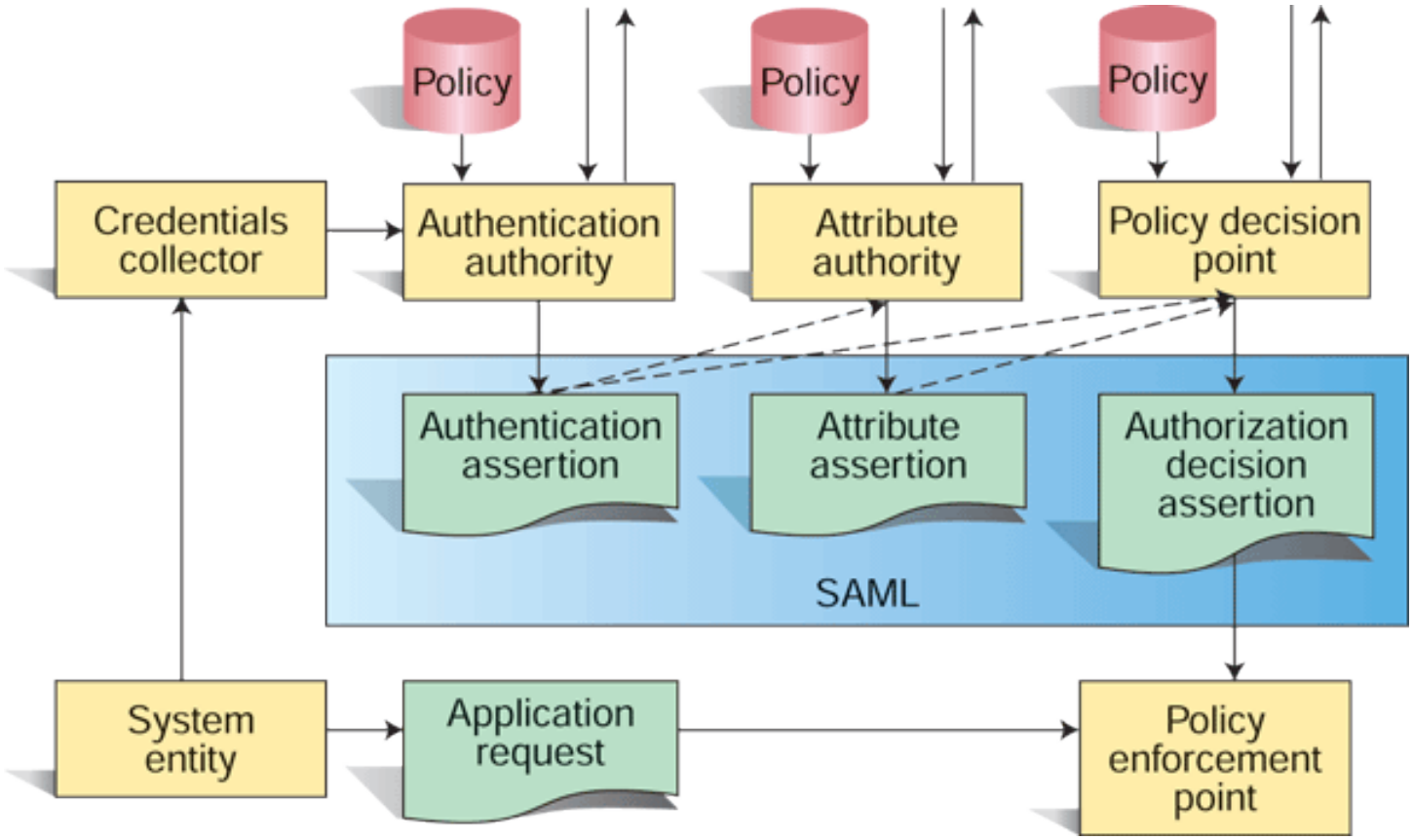
PENNSTATE

SAML

- Security Assertion Markup Language
- A method of representing authentication and authorization data in XML
- The origin university signs the SAML assertion with an x.509 signing certificate
- Encryption can be provided by W3C's XML-Encryption standard or by transporting the assertion in an SSL wrapped protocol
- Any protocol can be used to transport the SAML assertion
- Developed by OASIS, Version 1.0 was released 11/6/2002
- Used by Shibboleth & Liberty Alliance

PENNSTATE

SAML Model



PENNSTATE

XML-Signature


```
<Response IssueInstant="2003-01-16T17:05:54Z" MajorVersion="1" MinorVersion="0"
Recipient="http://mearnest2.oas.psu.edu/shibboleth/SHIRE" ResponseID="23f27b5a-e834-497e-9b3b-cb9396dcb081">
 <ds:Signature>
  <ds:SignedInfo>
   <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
   </ds:CanonicalizationMethod>
   <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
   </ds:SignatureMethod>
   <ds:Reference URI="">
    <ds:Transforms>
     <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
     <xfilter2b:XPath Filter="intersect">here()/ancestor::samlp:Response[1]
     </xfilter2b:XPath>
     <xfilter2b:XPath Filter="subtract">here()/ancestor::ds:Signature[1]</xfilter2b:XPath>
    </ds:Transform>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    </ds:Transform>
   </ds:Transforms>
   <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
   </ds:DigestMethod>
   <ds:DigestValue>GmJUZuLvKjtsCMOi2kuaY/NWweE=</ds:DigestValue>
   </ds:Reference>
   </ds:SignedInfo>
<ds:SignatureValue>
mYRHcRCDA6T2QOlX30cpoujYIag9MxNOzPnVXkq576QoSM3BLqZht83YhqFQDOYgGq7bLv9udOVUo5ui6xmXQm2Fb2w0I1s
LnX5fA5LQViCb+TjYEItAfRLPme+fFNBo2tmQ/y3oFwodgbbXpdAYKkw5Eej+7E4m8b9PUaczYjp/xVTEQ9rfZVyNW3wbCY/Ug
Ul79+hnvqKYPoBM7GK59lf9nF7WGSUMtXMoh+vei9kiScWoBFh0wAIJB9rbyFZGPm88MI0Qg9OZnRqHFVCQGGLtTxSXsKgD
v8H6TnaEeZgRVatTyGguMDw9dETAjUTGkBNTY8NDZm/haTi4WLhj/g==
</ds:SignatureValue>
```

XML-Certificate


```
<ds:KeyInfo>
  <ds:X509Data>
  <ds:X509Certificate>
MIIF4TCCBMmgAwIBAgIBRjANBgkqhkiG9w0BAQQFADCB0DELMAkGA1UEBhMCVVMxFTATBgNVBAgT
DFBlbm5zeWx2YW5pYTEYMBYGA1UEBxMPVW5pdmVyc2l0eSBQYXJrMSowKAYDVQQKEyFUaGUgUGVu
bnN5bHZhbmlhIFN0YXRlIFVuaXZlcnNpdHkxKDAmBgNVBAsTH0luZm9ybWF0aW9uIFRlY2hub2xv
Z3kgU2VydmljZXMxHDAaBgNVBAMTE1BLSSBFdmFsdWF0aW9uIFRlYW0xHDAaBgkqhkiG9w0BCQEW
DXBzdWNhQHBzdS5lZHUwHhcNMDMwMTA3MjExNzA4WhcNMDQwMTA3MjExNzA4WjCBzjELMAkGA1UE
BhMCVVMxFTATBgNVBAgTDFBlbm5zeWx2YW5pYTEYMBYGA1UEBxMPVW5pdmVyc2l0eSBQYXJrMSow
KAYDVQQKEyFUaGUgUGVubnN5bHZhbmlhIFN0YXRlIFVuaXZlcnNpdHkxKDAmBgNVBAsTH0luZm9y
bWF0aW9uIFRlY2hub2xvZ3kgU2VydmljZXMxGjAYBgNVBAMTEWJzb2QuYXNldC5wc3UuZWR1MRww
BglghkgBhvhCAQgEMBYuaHR0cDovL3d3dy5jcmVuLm5ldC9jcmVuY2EvZG9jcy9wa2lsaXRlY3Bz
LnBkZjALBgNVHQ8EBAMCBaAwGAYDVR0RBBEwD4ENbXhlMjBAcHN1LmVkdTAdBgNVHQ4EFgQUul2G
eIfBWLVqD/WVseKVdiyNOZgwgfEGA1UdIwSB6TCB5oAUyqL/0EDxVxDinYXH/cz5k6Ubb8Whgcqk
gccwgcQxCzAJBgNVBAYTAlVTMRUwEwYDVQQIEwxQZW5uc3lsdmFuaWExGDAWBgNVBAcTD1VuaXZl
cnNpdHkgUGFyazEqMCgGA1UEChMhVGhlIFBlbm5zeWx2YW5pYSBTdGF0ZSBVbml2ZXJzaXR5MSgw
JgYDVQQLEx9JbmZvcm1hdGlvbiBUZWNobm9sb2d5IFNlcnZpY2VzMRAwDgYDVQQDEwdwc3UuZWR1
MRwwGgYJKoZIhvcNAQkBFg1wc3VjYUBwc3UuZWR1ggE/MBEGCWCGSAGG+EIBAQQEAwIGwDAnBgNV
HSUEIDAeBggrBgEFBQcDAQYIKwYBBQUHAwIGCCsGAQUFBwMDMA0GCSqGSIb3DQEBBAUAA4IBAQCZ
+8RL0wxSatgxdW5jzbsiGD8gMGUmp20vNg3cvtVNa2VRL34ZpvNEJVvkYrsQOFwCrsmHd57n7eHH
VAfPKboa4XPj15aiHhdOi8mEFMzAUN7mDnryBGYXP+KU7+xj7g9Eke1dkfQQBzSCyb/95YhHj90V
f6KuVwKNgIikN2NeeA5xGPR7uCYDqNso1jKr+OBJh7JGo2y4JVa/DL2/pTL3Y7oxEmLsZc/0prux
VR3/U1qrANUpKsPfQZBdbCplbygi7cvHEp/RNC56PF2guG9P9GWm57uqo6TWxIIAfEiWIE0H2G9T
Y9WPxytcdJo1mh75Vh6ZNLXGy1Kcsd6KLyU7
  </ds:X509Certificate>
  </ds:X509Data>
 </ds:KeyInfo>
</ds:Signature>
```

PENNSTATE

Authentication Assertion

```
<Status>
 <StatusCode Value="samlp:Success"></StatusCode>
</Status>
<Assertion AssertionID="35035173-6a21-47e0-8fd8-d8ab3a6a3aac" IssueInstant="2003-01- 16T17:05:54Z"
Issuer="bsod.aset.psu.edu" MajorVersion="1" MinorVersion="0">
 <Conditions NotBefore="2003-01-16T17:05:54Z" NotOnOrAfter="2003-01-16T17:10:54Z">
  <AudienceRestrictionCondition>
   <Audience>http://middleware.internet2.edu/shibboleth/clubs/clubshib/2002/05/
   </Audience>
  </AudienceRestrictionCondition>
 </Conditions>
 <AuthenticationStatement AuthenticationInstant="2003-01-16T17:05:54Z" AuthenticationMethod="Basic">
  <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>
   <SubjectLocality IPAddress="146.186.121.40">
   </SubjectLocality>
   <AuthorityBinding AuthorityKind="samlp:AttributeQuery" Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-
binding"    Location="https://bsod.aset.psu.edu/shibboleth/servlet/AA">
   </AuthorityBinding>
  </AuthenticationStatement>
 </Assertion>
</Response>
```

PENNSTATE

Attribute 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>
```

PENNSTATE

OpenSAML

- Set of Java and C++ classes to build, transport and parse SAML assertions
- Implements HTTP-POST and SOAP to transport SAML Assertions (more are planned)
- Developed by Internet2 Middleware team to support Shibboleth
- Provides a simple API for applications to make use of SAML Security
- Tested and used on Windows 2000/XP, Linux, and Solaris
- Open Source under the OpenSAML license (Based on MIT License)
- www.opensaml.org

PENNSTATE

Shibboleth

- Architecture to provide inter-realm authentication and authorization with emphasis on user privacy
- Utilizes eduPerson, SAML, and OpenSAML
- Provides secure exchange of interoperable attributes which can be used in access control decisions
- Designed to work with existing systems requiring as little change as possible.
- Co-developed by Internet2/MACE and IBM/Tivoli
- Open Source (also based on MIT License)

PENNSTATE

Shibboleth Concepts

- Target Site
  - The protected resource the user wishes to access
  - Consists of Resource Manager, SHIRE, and SHAR
  - Where authorization rules reside and access decisions are made
  - Receives all information about the user from the Origin Site
- Origin Site
  - Where the user's attributes, authentication database, and attribute release policy are located
  - Consists of the Handle Service, Attribute Authority, and Attribute Release policy
  - Asserts identity and attributes of the user to the Target Site
- WAYF (Where Are You From) Server
  - Queries user to determine what institution they are from
  - Redirects them to their Origin Site's Handle Service
  - Can be a separate server, or part of the Target Site

PENNSTATE

Origin Site Components

- Handle Server
  - Works with local authentication system to authenticate user
  - Generates an opaque handle to identify user
  - Maintains a mapping from the opaque handle to the user's identity
  - Responds to an Attribute Query Handle Request
  - Sends Authentication SAML assertion to the Target Server's SHIRE component
- Attribute Authority
  - Works with local directory to acquire user attributes
  - Uses the Attribute Release Policy to determine which attributes can be released
  - Responds to an Attribute Query Message from the SHAR
  - Sends Authorization SAML Assertion to Target Site's SHAR component
- Attribute Release Policy
  - Specifies rules for what attributes are to be released to which Target Site
  - Can also be user specific and user controlled

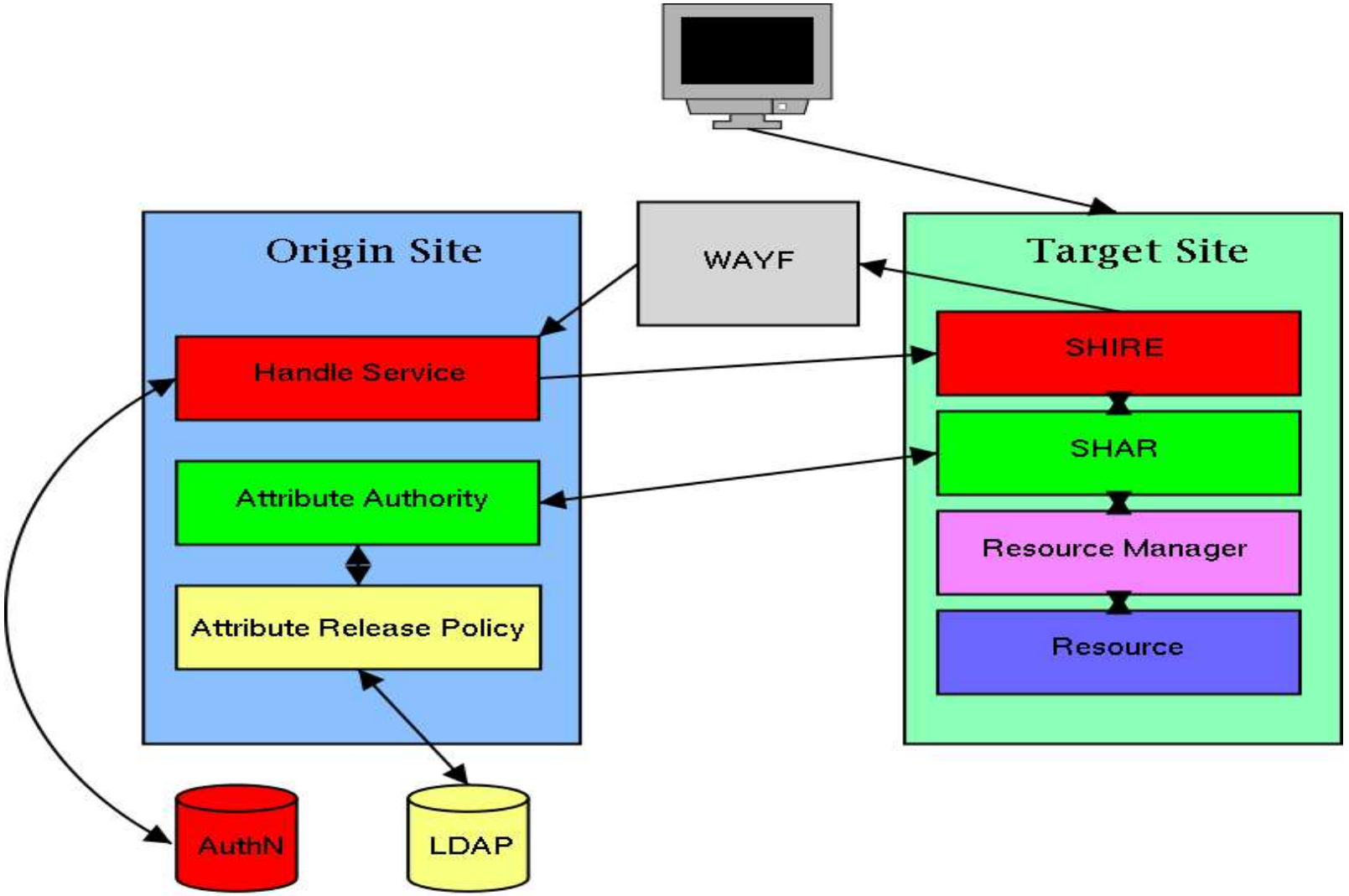
PENNSTATE

Target Site Components

- SHIRE
  - SHibboleth Indexical Reference Establisher
  - Accepts and validates Authentication SAML assertions from Handle Service
  - Associates the opaque handle with a session it creates
  - Passes control to the SHAR
- SHAR
  - SHibboleth Attribute Requester
  - Using the opaque handle from the SHIRE, requests attributes from the Attribute Authority, then passes them to the Resource Manager
- Resource Manager
  - Accepts attributes from the SHAR
  - Makes authorization decisions based on local rules and the user's Attributes

PENNSTATE

Shibboleth Model



PENNSTATE

Shibboleth Principles

- Authentication system agnostic
  - Authentication is handled by the web server at the Origin Site
- Open Source & Open Standards
  - No vendor suppled software is required
  - All protocols and messages are documented RFC-style
- Active privacy protection
  - End user can dictate which attributes are released to which Target
  - No identifying attributes (example: username) are sent by default
- Security
  - x.509 certificates assure validity of SAML assertions
  - Encryption may be employed in a variety of ways (XML-encryption, SSL, etc)
  - Builds on existing campus security archecture instead of replacing it.

PENNSTATE

Shibboleth Requirements

- SSL Web Server
  - Apache 1.3.x (Apache 2.x support is being worked on)
  - IIS 5 or later
- LDAP Server
- Tomcat Application engine (Origin Site)
- Java Runtime Environment (Origin Site)
- Digital Certificate with DigitalSignature attribute
- OpenSSL
- Log4cpp
- Libapreq, libxml2, libxslt, xmlsec

PENNSTATE

References

Graphics and text from the following resources were used in the development of this presentation.

- eduPerson Specification
  - http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduPerson-200210.pdf
- SAML 1.0 Assertions and Protocol
  - http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf
- OpenSAML FAQ
  - http://www.opensaml.org/faq.html
- Shibboleth Update -- Ken Klingenstein
  - http://middleware.internet2.edu/shibboleth/presentations/Shib-ALA4.ppt
- Shibboleth Update - Steven Carmody
  - http://shibboleth.internet2.edu/presentations/shib-acamp731.htm