

Shibboleth 2.0

Nate Klingenstein

Internet2

EuroCAMP 2007 Helsinki

April 17, 2007



Overview

- Timeline
- A few concepts
 - Protocols
 - Attributes
 - Other changes
- A few examples
 - Configuration preview



Timeline

- Tech Preview of AA released mid-March
- Beta scheduled for public availability at the end of May
 - Native SP
 - Java IdP
 - Java SP TBD, but not much coding left
- Full release when we're confident it's mostly bug-free



Shibboleth Protocol Changes

- Attribute push will be the default
 - Encrypted assertions
 - Encrypted requests
- TLS authentication for back-channel calls
 - Port 8443 only needed in limited circumstances
- Provider internals protocol-agnostic
- Most of SAML 2.0, ADFS, SAML 1.1 / Shibboleth 1.x; other protocols soon



Metadata

- Encryption of requests that pass through the browser require a key to use
- So do unsolicited assertions (IdP-first, portal, etc.)
- Some form of the provider's key must be present in metadata
 - Alternative is relying on secure channels or callbacks



The New Attribute

- Uniform internal attribute ID
- IdP Attribute Lifecycle:
 - Gathered from source by attribute resolver
 - Transformed by attribute resolver
 - Filtered through attribute filters (ARP's)
 - Encoded by attribute encoders
- SP uses same process (mostly) in reverse



Attribute Resolver

- It's not just for IdP's anymore
 - Native SP, Java SP, Java IdP all have one
- Multiple attribute sources
 - JDBC, JNDI, etc.
 - Received assertions are a source too
- Very powerful Java scripting engine
 - Apache's Velocity



Attribute Filters

- Replace AAP's and ARP's
- A filter is active when the policy statements within it are matched
- Rules within that filter are then applied to inbound/outbound attributes
- Policies may be written based on almost anything, including:
 - Providers
 - Principals
 - Other Attributes



Attribute Codecs

- Attributes are named by a friendly internal ID throughout the provider
- Encoders are attached to the attribute by the provider
- When an attribute is ready to send, the protocol handler selects its encoder to prepare the attribute for transport
- When an attribute is received, a decoder translates it back into an internal form



Native SP State

- Native SP now has an ODBC backend for management of persistent data
 - Replay cache
 - Session cache
 - Artifacts (for request storage)
 - Logout
- Multiple assertions per session supported
- Raw assertions exposed



User Authentication

- The IdP must interpret an AuthnRequest before deciding how to authenticate a user
 - isPassive
 - Requested Methods
- Unless your AuthN service wants to parse SAML, IdP must handle the request first
- Shibboleth 2.0 will ship with built-in simple authentication handlers; several functional layers
 - API to allow for custom interfaces by your authn system



Configuration Examples

- shibboleth.xml
- resolver.xml
- policy.xml

