Shibboleth Update

Internet2 Spring Member Meeting

Scott Cantor
cantor.2@osu.edu
Chad La Joie
lajoie@itumi.biz
Nicole Harris
nicole@shibboleth.net

Consortium: Website

- New website: http://shibboleth.net

Consortium: Developers

- Current Developers: 2 FTE - Brent (800h), Chad (1400h), Ian (300h), Rod (400h), Scott (450h)
- Current allocation
  - 45% project support, overhead, standards development
  - 25% product maintenance
  - 35% new product development (.5FTE)
- Current level of development resources do not allow for committed timelines on new releases

Consortium: Joining

- Membership now open - both proposed levels and donations to the Consortium welcomed
- Short membership agreement (5 bullets), supporting a Membership Charter
- Additional members would allow us to produce new releases/products faster and commit to timelines

Current Software

Current Software

- Identity Provider
  - current release: 2.3.6
  - last 6 months: security/bug fix releases

Current Software

- Identity Provider
  - current release: 2.3.6
  - last 6 months: security/bug fix releases
- OpenSAML
  - current release: 2.5.3
  - last 6 months: bug fix releases

Current Software

- Centralized Discovery Service
  - current release: 1.2.1
  - last 6 months: feature and bug fix releases
    - improved metadata loading features - close to parity with IdP
    - improved encoding of content
- no more feature releases in 1.x line
  - just bug fixes from here on out
  - if the CDS is important to you, convey that to the Consortium

Current Software

Current Software

- Embedded Discovery Service
  - current release: 1.0.2
  - last 6 months: bug fix releases
    - corrected some encoding issues
    - added Japanese localization (thanks GakuNin!)
- still time to provide other localizations before 1.1

Current Software

- Embedded Discovery Service
  - current release: 1.0.2
  - last 6 months: bug fix releases
    - corrected some encoding issues
    - added Japanese localization (thanks GakuNin!)
  - still time to provide other localizations before 1.1
- Service Provider
  - current release: 2.4.3
  - last 6 months: bug/security fixes

Metadata Aggregator

- Current release: 0.7
  - some new features, mostly a port to java-support lib
- Plans for 0.8
  - entity attributes: creating and filtering
  - command line support for configuration macros
  - full list can be found in Jira
- More testers and feedback would be good
- Github repository for Metadata Query Protocol

https://github.com/lajoie/mq-query

OpenSAML v3

OpenSAML v3

- Multi-module Project:
  - merged xmltooling, openws, opensaml v2 libraries
  - broken apart in to smaller modules - allows smaller deploying footprint

OpenSAML v3

- Multi-module Project:
  - merged xmltooling, openws, opensaml v2 libraries
  - broken apart in to smaller modules - allows smaller deploying footprint
- Bootstrap Configuration
  - bootstrap configuration files located in JARs
  - configured via Java Services API
  - just call init method and magic happens

OpenSAML v3

- Multi-module Project:
  - merged xmltooling, openws, opensaml v2 libraries
  - broken apart in to smaller modules - allows smaller deploying footprint
- Bootstrap Configuration
  - bootstrap configuration files located in JARs
  - configured via Java Services API
  - just call init method and magic happens
- Validator classes have been removed

OpenSAML v3

OpenSAML v3

- Context API
  - generic tree structure of type-safe, named data
  - replaces message context and IdP profile contexts
  - no more 15-level deep class hierarchies for state data

OpenSAML v3

- Context API
  - generic tree structure of type-safe, named data
  - replaces message context and IdP profile contexts
  - no more 15-level deep class hierarchies for state data
- Metadata APIs
  - broken in to two parts
  - **metadata provider** - brings metadata in to the system
  - **metadata resolver** - searches pool(s) of metadata

IdP v3

IdP v3

- Attribute resolver and filtering engine
  - core code completed and tested
  - most plugins completed and tested - database and LDAP resolver plugins still need to be done

IdP v3

- Attribute resolver and filtering engine
  - core code completed and tested
  - most plugins completed and tested - database and LDAP resolver plugins still need to be done
- Profile handling code
  - about 25% done
  - most individual actions identified, some written, none tested

IdP v3

- Attribute resolver and filtering engine
  - core code completed and tested
  - most plugins completed and tested - database and LDAP resolver plugins still need to be done
- Profile handling code
  - about 25% done
  - most individual actions identified, some written, none tested
- Authentication main focus of current development

IdP v3: Authn: Concept

IdP v3: Authn: Concept

- Authentication is a workflow of discrete actions

IdP v3: Authn: Concept

- Authentication is a workflow of discrete actions
- An action transitions to one of any number of other actions based on return value/exception

IdP v3: Authn: Concept

- Authentication is a workflow of discrete actions
- An action transitions to one of any number of other actions based on return value/exception
- Process is done when a “finalize” step is called

IdP v3: Authn: Concept

- Authentication is a workflow of discrete actions
- An action transitions to one of any number of other actions based on return value/exception
- Process is done when a “finalize” step is called
- General process includes three steps:
  - request for / collection of credentials
  - extraction of credentials from transport
  - validation of credentials

IdP v3: Authn: Mechanisms

IdP v3: Authn: Mechanisms

- Username/Password
  - collection: display page, basic auth request
  - extraction: response fields, WSS tokens
  - validation: LDAP, Kerberos domain

IdP v3: Authn: Mechanisms

- Username/Password
  - collection: display page, basic auth request
  - extraction: response fields, WSS tokens
  - validation: LDAP, Kerberos domain
- IP Address
  - extraction: request fields
  - validation: configured CIDR blocks

IdP v3: Authn: Mechanisms

IdP v3: Authn: Mechanisms

- Kerberos
  - collection: SPNEGO request
  - extraction: response fields
  - validation: Kerberos domain

IdP v3: Authn: Mechanisms

- Kerberos
  - collection: SPNEGO request
  - extraction: response fields
  - validation: Kerberos domain
- X.509 Certificates
  - extraction: TLS connection, WSS token
  - validation: OpenSAML trust engines

IdP v3: Authn: Mechanisms

- Kerberos
  - collection: SPNEGO request
  - extraction: response fields
  - validation: Kerberos domain
- X.509 Certificates
  - extraction: TLS connection, WSS token
  - validation: OpenSAML trust engines
- Existing Session

IdP v3: Authn

IdP v3: Authn

- v3 will ship with example workflows that mimic current v2 functionality

IdP v3: Authn

- v3 will ship with example workflows that mimic current v2 functionality
- Supports chaining/failover mechanism, injection of policy/Terms of Use

IdP v3: Authn

- v3 will ship with example workflows that mimic current v2 functionality
- Supports chaining/failover mechanism, injection of policy/Terms of Use
- All displayed pages are Velocity templates and exist outside the WAR file
  - can be changed without restarting the IdP
  - aren’t overwritten during upgrades

IdP v3: Authn

- v3 will ship with example workflows that mimic current v2 functionality
- Supports chaining/failover mechanism, injection of policy/Terms of Use
- All displayed pages are Velocity templates and exist outside the WAR file
  - can be changed without restarting the IdP
  - aren't overwritten during upgrades
- Added extensibility means added complexity/ configuration

SP v2.5

- Full list of bug fixes and feature additions in Jira
- Alpha RPM releases available from download repo
- Targeting a summer release
- Significant note: Solaris build will be “hard” due to limitations of platform/compiler
  - gcc may become a better choice

https://issues.shibboleth.net/jira/secure/IssueNavigator.jspa?requestId=10034
http://download.opensuse.org/repositories/home:/Scott_Cantor/

SP v2.5: Packaging

- Run as non-root (done)
- Version-independent web content (done)
- Protect conf.d/shib.conf Apache settings (done)
- Init script support for /etc/sysconfig/shibd (done)
- Working towards Windows upgrade support (expected)

SP v2.5: Audit Logging

- Backward compatible if not specially configured
- Deployer-selected fields, format, delimiters, etc.
- Open to input on new defaults

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLogging

SP v2.5: Error Handling

- Leverage information about attributes required by a service
- Validate requirements at login time before transfer of control back to resources
- Handle missing attributes with customized error responses

SP v2.5: Error Handling

- New plugins that extract info from metadata: error URL, contacts, descriptions, policy links
  - Metadata AttributeExtractor
- Post-login validation
  - generic “sessionHook” feature
  - “Attribute Checker” endpoint
    <Handler type=”AttributeChecker” Location=”/AttrChecker” attributes=”eppn displayName” template=”attrChecker.html” flushSession=”true” />

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler

Attribute Munging

- Transform AttributeResolver

```
<AttributeResolver type="Transform" source="displayName">
   <Regex match="^(.+)(.+)$" dest="givenName">$1</Regex>
   <Regex match=" ^(.+)(.+)$" dest="sn">$2</Regex>
</AttributeResolver>
```

- Template AttributeResolver

```
<AttributeResolver type="Template" source="givenName sn" dest="displayName">
   <Template>$givenName $sn</Template>
</AttributeResolver>
```

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeResolver

SP v2.5: Back Door Integration

- OpenID Connect no supported yet
  - since it's so easy, you can do it
- Two Mechanisms
  - generate a SAML ArtifactResponse message in a file; generate a matching artifact for the client to submit using SAML artifact binding
  - generate a SAML Assertion and submit to http://localhost/Shibboleth.sso/ExternalAuth from a server-side script, get back a session cookie to give to client

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPBackDoor