Shibboleth Roadmap

Shibboleth Consortium Roadmap

- Committed Work
  - necessary/expected ongoing functions
  - funded/staffed projects
- Planned Work
  - accepted for prioritization but not yet started
- Under Discussion
- Rejected/Parked Work
  - lacking in some regard
  - subject to re-evaluation when circumstances change or requirements crystallize

Committed

- Project Overhead
- Standards Development
- User Support
- Supported Release Maintenance
  - note: minor point releases **become** the supported release (e.g. SP 2.4, IdP 2.2)
- IdP 2.3 and IdP / OpenSAML-J 3.0
- Embedded Discovery Service 1.0
- Metadata Aggregator 1.0

Planned

- Expanded introductory documentation
- V2 Centralized Discovery Service
- V3 TestShib
- Back-channel SAML Logout for the IdP
- Second Factor Authentication via SMS
- SP Delegation / Web Service Enhancements

SP Roadmap

https://spaces.internet2.edu/display/SHIB2/SPRoadmap

- Identifies current/next/future releases along with links to bug/RFE lists
- In-depth summaries or links to topics describing specific features under discussion or development
- Basically, anything that's hard to represent in Jira...
- Any feature discussions happen via dev mailing list

Current Release (2.4.2)

- Suggested for everybody; critical on Linux
  - bug in User-Agent feature generates HTTP 400 errors on SOAP queries
- Upgrade from 2.3 otherwise very stable
- Shorter/simpler configuration
- Metadata caching and background reloads
- Blacklisting of weak cryptography algorithms

Future Release

- 2.5 vs. 3.0
- Extensions
  - keep piling on or package separately?
  - attribute resolver functionality (data munging, scripting?)
  - delegation / web service improvements
- Revamp audit logging
- Handling attribute requirements / detecting errors / privacy disclosures
- Discovery “lessons learned” improvements

Web Service Delegation

- “Early access” feature relying on IdP extension and a non-trivial custom HTTP library
- Browser → web site → web service flow relies on a lot of middle-tier SP information:
  - which IdP was used and its public key(s)
  - where/how to contact IdP extension endpoint
  - user's SSO token from IdP
  - SP's private key

Web Service Delegation cont.

- Goal: design an extension to eliminate sharing of state between SP and WS client library
- Secondary goal: offload (relative) complexity of client/IdP SOAP interaction to SP
- Tertiary goals:
  - relieve WS client of all non-HTTP responsibility by proxying web service access?
  - insulate client from WS security mechanism?
  - perhaps allow seamless integration of OAuth?

Provisioning Application Integration

- Weird idea in the early thought balloon stage: facilitate deployment of application plugins designed around SP
- A few cases in point: Confluence/Jira, Drupal, LMS tools
- Can we abstract the integration points with the SP into something expressible in XML or JSON to provision with?
  - headers/variables to access, SSO request initiation, logout, discovery, …?
  - maybe it's a two-way communication...
  - maybe this is an insane, hopeless idea...
- Definitely would require joint discussion/buy-in.

Embedded Discovery Service

- New Discovery Service meant to be co-resident with Service Provider
- Consumes data from SP 2.4+
- Enabled by adding:
  - one
  - one CSS <link>
  - two <script>s
- Currently in beta, 1.0 to be released soon

Centralized Discovery Service

- Current v1.1.2 released 12-Jan-2011
  - minor bug fix release
- 2.0 code rev
  - make it look like other Shib Java projects
    - similar installation, configuration, dependencies
  - produce JSON feed used by Embedded DS
  - use Embedded DS as UI
  - better APIs for filtering and sorting IdPs
  - distributed with a configured servlet container

Identity Provider 2.3

- IdP Initiated SSO
  - uses Shib SSO protocol but works for SAML 2
- Dynamic Metadata Provider
  - just-in-time entity metadata fetching
- Entity Attributes based Attribute Filtering
  - “tag” metadata entities with SAML attribute
  - use those attributes in attribute filtering policy
- Misc. small improvements and bug fixes

IdP 3.0: Main Goals

- Support in-flow extensions to protocol processing
  - e.g., terms of use, attribute consent
- More flexibility in Authentication process
  - separate credential extraction from validation
  - bubble up better errors to users
  - multi-factor or multi-step authentication
- In-place upgrade of configuration files
  - except for custom developed extensions and JSPs

IdP 3.0: Other Features

- Authentication: SPNEGO, non-browser
  - support SOAP w/ password, X.509, SAML token
- Conditional evaluation of attribute resolution components
- Out of the box attribute consent engine
  - similar to uApprove but with a few extras
- Profile handler extensions merged in:
  - delegation, ECP, back-channel single logout
- Metadata guided crypto algorithm selection

IdP 3.0: Other Features

- Reduced configuration files
- Performance metrics for various components:
  - attribute resolver, filter engine, authentication, etc.
- HA-Shib like clustering:
  - reduced configuration
  - no external process to manage/monitor
  - provides clustered data store
- Shipped with installer-configured container

Metadata Aggregator

- Tool for munging and querying metadata
- Use Cases:
  - Federations collect, check, and compile metadata
  - Local institutions may want to:
    - pre-process and proxy federation metadata (e.g., offload signature validation)
    - merge in their local metadata
  - Inter-federation requires merging, transforming, and reforming metadata from multiple sources

Metadata Aggregator

- What checks/transformations?
  - XML: schema validation, signature creation/validation, XSLT transformation
  - SAML: filter entity, role, organization and contact person, manage cacheDuration and validUntil
- Two interfaces
  - command line tool for single-shot or scripted use
  - HTTP web service interface for queries