Shibboleth Identity Provider 3.0

Recent developments and current status

SWITCH

SWITCHaai Team
aai@switch.ch

IdP v3 Development Timeline

- work on design document begun in 2011
- development with new team members intensified in 2013
- version 3.0.0-alpha1 released on 26 June 2014
- version 3.0.0-alpha2 released on 29 July 2014
- release currently scheduled for Q3 2014 (“betas in the late summer time frame”) … may further shift, though

IdP v3 Main Goals

- “to create a more modular platform that makes customizing profile flows and many other behaviors simpler with less code”
- “remove most/all SAML dependencies from the core of the platform”

https://wiki.shibboleth.net/confluence/display/DEV/IdP3Details

IdP v3 What's New

- will include features which were only available as separate extensions for the IdP v2:
  - user consent for attribute release (uApprove) *
  - support for SAML ECP ("Enhanced Client or Proxy") profile without the need for container-based authentication
  - X.509 certificate based authentication *
- more flexible configuration
  - native Spring XML configuration
  - Velocity templates which support on-the-fly modification of UI pages (in contrast to JSP pages, which require a container restart)
- support for stateless clustering
  - uses client-side (cookie) session storage by default

* not yet implemented in the alpha versions released so far

IdP v3 Requirements

- Java 7 or later
  - incompatibilities with the JavaScript engine in Java 8 (“Nashorn”), which is used for script-based attribute definitions (for Java versions up to 7, the “Rhino” engine is used)
- servlet container with Servlet API 3.0 support, such as
  - Tomcat 7 or later
  - Jetty 8 or later

Note: the IdP v3 will *not run* with Java or servlet container versions older than those listed above.

IdP v3 Backward Compatibility

- v3 feature set is a superset of v2
- keeping existing configuration files from v2 is partly supported:
  - **`relying-party.xml`** (deprecated, migration to new configuration syntax is recommended, in particular for using new/advanced features)
  - **`attribute-resolver.xml`** (some parts deprecated: **`<PrincipalConnector>`** elements and NameID encoders)
  - **`attribute-filter.xml`** (with the exception of four **`AttributeIssuer`** rules)
- authentication component fundamentally redesigned
  - based on Spring Web Flows (SWF), configuration completely new
  - login handlers for IdP v2 need to be adapted/rewritten

Current status and outlook

- initial alpha release tests at SWITCH in July/August
  - OpenJDK 7, Tomcat 7, Apache httpd 2.2 + mod_proxy_ajp
  - some hickups with alpha1 (mostly addressed in alpha2)
  - basic features (SAML 2 Web Browser SSO, LDAP backend for authentication and attribute resolution, SQL backend for persistent ID) is working fine
  - user consent and X.509 authentication not yet implemented
- more testers from the community welcome
  - see https://wiki.shibboleth.net/confluence/display/IDP30/Home
  - documentation is relatively sparse, for the time being (familiarity with IdP v2 configuration required)
- SWITCH will overhaul its deployment and upgrade guides for IdP v3