Shibboleth 2 IdP

What's new in the minor versions?

SWITCH

Serving Swiss Universities

Kaspar Brand
kaspar.brand@switch.ch

Berne, 24 May 2011

Shibboleth IdP 2.x timeline

2.0.0: released March 2008

2.1.0: released November 2008

2.2.0: released September 2010

2.3.0: released May 2011

[3.0: “when it’s ready”™]

1.x: end of life as of 1st July 2010
(no longer supported, last version released November 2009)

Shibboleth IdP 2.1 (November 2008)

- ability to store configuration files in Subversion or pull them from HTTP locations
- resource configuration file filters (first to be available: *PropertyReplacement,* replaces macros based on property files)
- introduction of an explicit *DenyValueRule* in the attribute filter policy
- addition of the BeanShell, Groovy, JRuby, and Jython scripting engines, for use in the Scriplet attribute definitions and filter rules

Shibboleth IdP 2.2 (September 2010)

- metadata provider improvements
  - reloading metadata in a background thread (prevents the most common cause of the occasional “pause” users see when logging in)
  - use of conditional HTTP GETs when pulling metadata from HTTP sites
  - support for HTTP compression
  - support for HTTP proxies
- LDAP improvements
  - LDAP result caching can now be enabled
  - improved failover capabilities when using multiple LDAP servers
  - option to lowercase attribute IDs that come from LDAP (addresses case-sensitivity issues encountered by some sites)
- changes in the syntax for specifying durations
  - XML Schema *duration* instead specifying milliseconds with integers

Shibboleth IdP 2.3 (May 2011) 1/2

- taglib support for rendering MDUI info on the login page (Metadata Extensions for Login and Discovery User Interface)
  - improves information for the user about the resource he is trying to access
- support for the ECP profile (Enhanced Client or Proxy)
  - previously only available as a separate extension, for non-browser based applications
- SAML 2, IdP-initiated SSO
  - modeled after the Shib SSO protocol used for SAML1
- new “external authn system” login handler
  - comparable to REMOTE_USER, but with additional flexibility

Shibboleth IdP 2.3 (May 2011) 2/2

- new attribute filtering options
  - based on name ID format (**`*NameIDFormatExactMatch`** rules)
  - based on entity attributes (**`*EntityAttributeRegexMatch`**)
- support for stateless IdPs if the artifact binding isn't used

  makes sure that all nodes generate the same transient IDs
- name ID prioritization, depending on the relying party

  configurable through the **`nameIDFormatPrecedence`** attribute
- more control over certificate validation (PKIX)
  - **`ValidationOptions`** child element in **`TrustEngine`** configuration
  - **`forceRevocationEnabled`** makes (successful) revocation checking mandatory

Should I upgrade?

- if you're running 2.0/2.1.x/2.2.x: **yes** – all releases are vulnerable to some form of cross-site scripting
  - releases prior to 2.1: login.jsp
    http://shibboleth.internet2.edu/secadv/secadv_20081103.txt
  - releases prior to 2.2: error.jsp
    shibboleth.internet2.edu/secadv/secadv_20090224.txt
    (can be fixed by editing the JSP page)
  - releases prior to 2.3: OpenSAML templates
    http://shibboleth.internet2.edu/secadv/secadv_20110516.txt
- cf. https://wiki.shibboleth.net/confluence/display/SHIB2/IdP22Upgrade for configuration related changes