What’s New in SAML 2.0?

Authored by Scott Cantor, The Ohio State University, and Chad La Joie, Georgetown University

NameID

- New Format Identifiers
  - Entity – SAML entity (e.g. IdP) identifier
  - Persistent – Opaque principal identifier; may be targeted to specific SP
  - Transient – Opaque, short lived, principal identifier
- Name ID Management
  - Allows SPs to request name IDs for particular formats
  - IdPs can inform SPs that an ID has changed
  - SPs can attach a local alias/secondary key to a persistent identifier

General Changes

- Incorporation of Shibboleth and Liberty SAML 1.X specifications and profiles
- Modularity and extensibility in schemas, profiles, and bindings
- Encryption support for specified elements; supports intermediary handling
- Refactoring of messages to reduce overall message size
- Stability of Specification; no new specification for a long time

Profiles

- Single Sign On
  - Request to log on to SP using an existing, established, authentication method
- Single Logout
  - Initiated (at IdP or SP) request logs user out of all SAML-aware services
- Enhanced Client/Proxy
  - SAML enabled client with knowledge of user’s IdP that supports SOAP-oriented bindings – no WAYF
- Attributes
  - X.500/LDAP – OID naming, octet string support
  - UUID/GUID – Special URN identifiers
  - DCE PAC – realm/cell and groups support

Authentication

- SP informs Authentication
  - Passive Authentication – client/browser can not take visible control (can’t look like you left SP)
  - Forced Authentication – requires authentication even if the user has authenticated before
  - Requested AuthN Context – requires that the user be authenticated with one of a list of particular methods
- Authentication Contexts
  - AuthN method – password, PKI, kerberos, SRP, ...
  - Environmental parameters – crypto challenge used, password length requirement

Metadata

- Describes SAML Entity services – single sign-on, attribute request, ...
- Defines groupings of Entities – equivalent to Shibboleth SiteGroups
- Provide contact and organization information about entities
- May be digitally signed for integrity checking
- Highly extensible
- Defined semantics for resolution via DNS NAPTR

Bindings

- HTTP POST
- HTTP Redirect
  - SAML Request/Response URL parameter encoded – prone to error due to URL length restrictions in many products
- SOAP 1.1
- PAOS
  - Liberty Reverse-SOAP send SOAP response on HTTP request and SOAP request on HTTP response – used by Enhanced Client/Proxy Profile
- Artifact
  - SAML Request/Response artifact transmitted via HTTP, resolved through back-channel

What’s New in SAML 2.0?

1. Logout Command
2. SAML 2.0 <LogoutRequest>
3. SAML 2.0 <LogoutResponse>
4. SAML 2.0 <LogoutResponse>
5. SAML 2.0 <LogoutResponse>
6. SAML 2.0 <LogoutResponse>

Single Logout Flow:

1. HTTP Request
2. <AuthnRequest> in HTTP Response
3. SAML 2.0 <AuthnRequest>
4. SAML 2.0 <AuthnResponse>
5. SAML 2.0 <AuthnResponse>
6. <AuthnResponse>

Enhanced Client/Proxy Flow:

1. ECP Enabled Client
2. SAML 2.0 <LogoutRequest>
3. SAML 2.0 <LogoutResponse>
4. SAML 2.0 <LogoutResponse>
5. SAML 2.0 <LogoutResponse>
6. SAML 2.0 <LogoutResponse>