Review of differences in SAML V2.0 from SAML V1.1 and ID-FF V1.2

Eve Maler
21 April 2004
Thanks to Scott and JohnK for comments
(line numbers are from sstc-saml-core-08-diff-from-02)
SAML V2.0 diffs in a nutshell

• Constitutes a large-scale realization in SAML of features derived from ID-FF V1.2, plus other requested features/fixes and some streamlining

• Backwards incompatibility is acceptable, if for a good cause

• Most backwards incompatibility is syntactic, not “semantic”
Planned SAML V2.0 schedule

- (All dates are approximate and may slip)
- Last-call draft review: Apr 30 to May 31
- Committee Draft review: Jun 30 to Jul 31
- OASIS Standard balloting: Aug 31 to Sep 30
Overview of diff categories

- Specs
- Versioning
- Subject
- Encryption
- Attribute
- Request/response
- Assertion retrieval protocol

- Session-related
- Federation
- Bindings and profiles
- Other
- Active work items
- Open issues

(Additions derived from ID-FF V1.2 features are in blue)
(Differences from ID-FF V1.2 are in red)
## Issues

Entry point for spec suite: Conformance spec or a new "cover spec"?

Worth it to create an image map of this graphic for the SAML home page (a la the Liberty Alliance spec page)?
Spec organization diffs

- Assertion and Procotol ("core") is now Assertion and Protocols
- Processing rules are now clearly called out in each protocol
- Bibliographic references have been divided into normative and non-normative (due to the ITU-T effort)
- Bindings and Profiles was split into two documents
- New Authentication Context, Authentication Context, and metadata specs
- New Baseline Attributes spec
Versioning diffs

- 338: **saml**: and **samlp**: namespaces now contain “2.0”
- 503 etc.: **MajorVersion** and **MinorVersion** attributes updated
- Backwards-incompatible changes planned during SAML V1.x have been made:
  - Deprecated **<AuthorityBinding>** has been removed
  - Deprecated **<RespondWith>** has been removed
  - Deprecated name identifier and artifact URIs have been removed
  - URI references are now required to be absolute
  - Cleaned up description of appearance of **<Status>** in SOAP messages
Subject and subject confirmation diffs

- 540: `<SubjectStatement>` goes away
- 573: `<Subject>` element moved up to `<Assertion>` and applied to all inner statements
  - And made optional to accommodate extensions like XACML's, though required in SAML's three statement types by means of spec prose (core-09)
- 953: `<ConfirmationMethod>` now just required, not repeatable
  - `<ds:KeyInfo>` now allowed only inside `<SubjectConfirmationData>` (core-09)
Encryption-related diffs

- 350: XML Encryption schema is imported
- 392: Name identifiers refactored to allow encryption
- (Several other blocks to be allowed to be encrypted, through work item W-9)
Attribute-related diffs

- 1085: `AttributeNamespace` goes away in favor of `NameFormat`, plus URIs for “unspecified” and “uri”
  - Now optional; default is “unspecified” (core-09)
- 1087: `AttributeName` changed to just `Name`
- 1095: New `ValueType` on `<Attribute>` and `<AttributeDesignator>`
  - To be removed?
- 1128: Arbitrary XML attributes allowed on `<Attribute>`
  - Also on `<AttributeDesignator>` for queries (core-09)
- 1122: Clearer instructions for null and multi-valued attributes
Request and response mechanism diffs

- 1548: Request type hierarchy reorganized; all queries are now *kinds* of requests, not inside requests; `<Query>` goes away as such
- 1339: Consent, `<RelayState>`, and `<Extensions>` added to all requests
  - Later removed `<RelayState>`; it's now a Bindings feature
- 478: Issuer now an element and based on name identifier
- 1383: Response type hierarchy reorganized; most `<Response>`s are simply of `StatusResponseType`
- 1479: New status codes to reflect new protocols
Assertion retrieval protocol diffs

- 1551: Instead of `<AssertionIDReference>` in `<Request>`, `<AssertionIDRequest>` now used to get an assertion by means of its ID

- 2272: Instead of `<AssertionArtifact>` to retrieve assertions in a response message, now a special protocol to get SAML protocol messages by means of an artifact
  - All types of protocol messages can theoretically be retrieved, but will be scoped down based on use cases

- 492: New AssertionURIReference element to go with new HTTP-based retrieval binding
Session-related diffs

- 806 and 1627: SessionIndex attribute added to <Statement> and <SubjectQuery>
  - SessionIndex is on all statements, not just <AuthenticationStatement>
- 2514: New Single Logout protocol
Federation-related diffs

- **1843**: New authentication request protocol
  - `NameIDPolicy` made more extensible than the old 4-way enumeration
  - `Subject` added to the request

- **993**: New `<AuthnContext>` in `<AuthenticationStatement>`

- **984**: `AuthenticationMethod` connected to `<AuthnContext>` through URI identifier
  - `AuthenticationMethod` may go away
  - Authentication context class schemas all changing

- **2363 and 2452**: New federated name registration and deregistration protocols
  - Now combined into a single federated name update protocol (core-10)

- **2639**: New name identifier mapping protocol
Bindings- and profile-related diffs

- New HTTP-based binding added for retrieval of assertions by means of URIs
- PAOS binding added
- ECP profile added
  - Uses a SOAP envelope, not a special XML envelope
- A lot of profile detail has been pushed down to become bindings; profiles are much thinner
  - E.g., there's an HTTP redirect/POST binding
  - URL encoding for this binding uses a general gzip method
- The two browser profiles are on track to become a single Web SSO profile
Other diffs

- 345 and 1301: XSD element substitution blocked
- 555: `<ds:Signature>` moved up in content model
  - Considering a request to move it to be first always
- 962: `<ds:KeyInfo>` usage updated subtly to allow more clearly for impersonation
- 1162 and 1732: `<AuthorizationDecisionStatement>` and `<AuthorizationDecisionQuery>` frozen
- 618 and 734: `<ProxyRestrictionCondition>` added to address Paul/Xavier comments
Active work items (as of sstc-saml-scope-2.0-draft-17)

- W-2a: SSO with Attribute Exchange
- W-4: Profile Enhancements for Metadata
- W-5: SSO Profile Enhancements
- W-6: Proxied SSO
- W-7: Discovery Protocol
- W-9: XML Encryption
- W-14: SAML Server Trust
- W-15: Delegation and Intermediaries
- W-25: Kerberos Support
- W-27: Security Analysis Enhancements
- W-30: Migration Paths
Open issues
(as of sstc-saml-2.0-issues-draft-08)

Priority A:
- CORE-11 Validity Period of Identifiers
- CORE-19 Multiple Encryption Keys and Recipient Information
- CORE-20 Change AuthnContextStatement Element Name
- BIND-3 Establish a Mandatory Profile
- TECH-2 Versioning of Elements
- TECH-3 Impersonation Using SubjectConfirmation and KeyInfo

Priority B:
- CORE-14 Indicating the Authority Binding
- CORE-16 Inconsistent Naming
- CORE-17 Bag of Conditions
- TECH-1 Identity/Service Provider Terminology and Domain Model
- TECH-4 Glossary Additions: Artifact, Binding, Profile

Priority C:
- CORE-7 SOAP Version in Protocol Binding
- CORE-8 Signing Assertions vs. Responses
- CORE-9 Wildcarding and Extensibility in the SAML Schemas
- CORE-12 Consider Changing Name Identifier Format Default for Issuer
- CORE-21 Consent vs. Reason
- CORE-22 URIs vs. Prefixed QNames in Status Codes
- CORE-23 Review Element vs. Attribute Choices
- TECH-5 Improve Federation Terminology
- TECH-6 Highlight Privacy Considerations