Advances in Oasis SAML and XACML

Standardized Federated Identity
Standardized Access Control

Anil Saldhana (Red Hat),
Oasis SAML TC Secretary and Oasis XACML TC Member
What is SAML?

- Security Assertion Markup Language (SAML) is a Oasis XML based standard for communicating user authentication, entitlements and attributes.
- SAML v2.0 is the latest ratified version.
- Widespread adoption in commercial products and open source products.
- Deployed in commercial, government, educational and non-profit environments.
Benefits of SAML

- Platform Independence.
- Loose coupling of directories.
- Seamless User Experience for users.
- Reduced administrative costs for Service Providers.
SAML Core Structure

- Core
  - AssertionID
  - Major Version
  - Minor Version
  - Issuer
  - IssueInstant

- Conditions
  - NotBefore
  - NotOnOrAfter
  - AudienceRestriction

- Statement (Authentication)
  - Subject
  - AuthnInstant

- Statement (Attribute)
  - Subject Attributes

- SAML Assertion

- XML Encryption

- XML Signatures
The Technical Committee since the publication of v2.0 has been working on erratas as well as the creation of multiple profiles.

- The TC has decided to update the v2.0 specifications this year to yield either SAML v2.1 or v2.0.1
- Approved errata to be integrated into core spec
- Some extensions/profiles will be merged into core spec
- HTML5 features into message bindings, logout.
- XML Signature v2.0
What is XACML?

- Oasis standard for representing and evaluating access control policies.
- Alternatives would be proprietary access control lists (ACL)
- XACML v2.0 is the current ratified version.

Widespread adoption in commercial and open source products
What is XACML?
Latest with XACML

- The Technical Committee is in the final phase of XACML v3.0 specification.
- Aim is to ratify the specification toward the end of this summer.
- XACML REST Profile (Work In Progress)
  - More load on the authorization server compared to authentication
  - ATOM or JSON Format
- XACML JSON Bindings (Brainstorm)
“Advice” has been introduced to broaden “Obligations”
- PEP may interpret advice and shall interpret obligation.
- Obligations can be part of rules now. Previously policies.
- New Profile: Administration and Delegation Profile.
- New Profile: Export Control US Profile.
Resources

- OASIS SAML Technical Committee Homepage
  http://www.oasis-open.org/committees/security/

- OASIS XACML Technical Committee Homepage
  http://wiki.oasis-open.org/committees/xacml/

Anil.Saldhana@redhat.com