International Telecommunication Union

SAML
Federated Identity at OASIS

Hal Lockhart

BEA Systems

ITU-T Workshop on "Digital Identity for NGN"
Geneva, 5 December 2006

ITU-T

SAML and the OASIS SSTC

- SAML: Security Assertion Markup Language
  - A framework for the exchange of security-related information between trusting parties
  - The key standard for federated identity systems
  - Supports many real-world business scenarios
  - Widely used today for cross-domain single sign-on
- OASIS Security Services Technical Committee (SSTC)
  - SSTC manages SAML development
  - 32 current voting members representing 22 organizations

ITU-T

Specification Suite

- Conformance Requirements
  - Required "Operational Modes" for SAML implementations
- Assertions and Protocols
  - The "Core" specification
- Bindings
  - Maps SAML messages onto common communications protocols
- Profiles
  - "How-to's" for using SAML to solve specific business problems
- Metadata
  - Configuration data for establishing agreements between SAML entities
- Authentication Context
  - Detailed descriptions of user authentication mechanisms
- Security and Privacy Considerations
  - Security and privacy analysis of SAML 2.0
- Glossary

ITU-T

SAML assertions

- Assertions are declarations of fact, according to someone
- SAML assertions are compounds of one or more of three kinds of “statement” about “subject” (human or program):
  - Authentication
  - Attribute
  - Authorization decision
- You can extend SAML to make your own kinds of assertions and statements
- Assertions can be digitally signed

ITU-T

SAML 2.0 Features

- Robust identity federation and management
- Enhanced web single sign-on profile
- Identity provider discovery
- Basic session management and global logout
- Encrypted attributes, name identifiers, and assertions
- Profiles for well-defined attribute sharing
- Fine-grained description of authentication mechanisms
- Metadata for simplified configuration
- Enhanced Client or Proxy (ECP) profile

ITU-T

Single-Sign On

- Browser-driven SSO
  - Form POST, SAML Artifact Profiles
    - Note: conformant implementations must implement both profiles
  - Assertions may contain attribute statements
    - SAML 2.0 introduces notion of attribute profile
  - All or certain parts of an assertion may be encrypted
    - Important when security intermediaries are involved
- SSO for enhanced client
  - Enhanced client is a device that understands HTTP but not SOAP
    - Also has “built in” knowledge of identity provider
  - Examples
    - HTTP proxies such as a WAP gateway
    - Consumer device with HTTP client

ITU-T

Identity Federation

- What is Identity Federation?
  - Agreement between providers concerning data used to identify users
    - User-specific attributes:
      - E-mail address?
      - Office number and Employee Id?
      - Role or membership in certain groups?
    - Unique, privacy-preserving identifiers known only to the providers?
  - Federated identifiers can be created in different ways
    - Dynamic assignment based on business agreements
    - Dynamic creation based on user consent
    - Out-of-band bulk synchronization or update at both parties

ITU-T

Identity Federation and Mgmt

- Multiple types of Name Identifiers
  - Well-known names
    - Email Address
    - X.509 Subject Name
    - Windows Domain Qualified Name
    - Kerberos Principal Name
  - Privacy-preserving pseudonym identifiers
    - Transient
    - Persistent
  - Name Identifier Management Protocol and Profile
    - Assign new pseudonym identifiers
    - Terminate identity federation

ITU-T

Anonymous user with attributes or roles

- User is never explicitly identified by a persistent identifier
  - A transient identifier is used as the "name" of the user
  - One or more roles or attributes describe the user
    - EmploymentLevel : Manager
    - AccessRights: Platinum
    - MemberOf: BellRingers
  - Access at Service Provider is given against roles or attributes
- No need to maintain user entry at SP
  - Privacy Preserving as user identity at IdP remains unknown
- Main use case in Shibboleth and some SAML 1.X deployments

ITU-T

User identified by privacy-preserving identifier

- User is identified by a persistent randomized string private to IdP and SP pairs
  - Unique handle per service provider
- Privacy-preserving since no information about user is available at SP
- Requires IdP and SP to synchronize portions of their user stores
- Affiliations: important sub-case where a single persistent randomized string is shared between a set of Service Providers
- Main use case in ID-FF 1.X specifications and deployments

ITU-T

Session Mgmt and Logout

- Session Participants
  - Identity Providers act as session authorities
  - Service Providers act as session participants
  - IdP defines session identifier(s) for SP's
  - User may initiate logout at IdP or SP to terminate session
  - User may terminate individual or all active sessions
- Follows ID-FF 1.2 closely (logout but no timeout) but also provides extension points for richer session models
  - Instructions for privacy preservation are provided

ITU-T

Standard Attribute Profiles

- Supports attribute naming and values drawn from a variety of syntaxes
  - Basic Attribute Profile: string names and attribute values drawn from XML schema primitive types
  - X.500/LDAP Attribute Profile: use of canonical X.500/LDAP attribute names and values
  - UUID Attribute Profile: Use of UUIDs as attribute names
  - XACML Attribute Profile: formats suitable for processing by XACML
- Attribute statements may be transferred during SSO or by the use of the AttributeQuery protocol
- Attributes may be encrypted to ensure end-to-end confidentiality

ITU-T

Name Identifier Management

- Protocol for communicating information about name identifiers
  - When identifiers should be updated
    - Replace jsmith@foo.com by johns@foo.com
    - Rollover privacy preserving identifier at SP every 6 months
    - Update identifier at IdP with identifier meaningful to SP
  - When an identifier will no longer be acceptable for federation
    - IdP will not issue any more assertions for jsmith@foo.com
    - SP will not accept assertions for jsmith@foo.com