What's New in SAML 2?

What's New in SAML V2.0?

- Pseudonyms - SAML V2.0 defines how an opaque pseudo-random identifier with no discernible correspondence with meaningful identifiers (for example, emails or account names) can be used between providers to represent principals. Pseudonyms are a key privacy-enabling technology because they inhibit collusion between multiple providers (as would be possible with a global identifier such as an email address).
- Identifier management - SAML V2.0 defines how two providers can establish and subsequently manage the pseudonym(s) for the principals for whom they are operating.
- Metadata - SAML's metadata specification defines how to express configuration and trust related data to make deployment of SAML systems easier. In doing this, it identifies the actors involved in the various profiles, such as SSO Identity Provider and Service Provider, and Attribute Authority and Requester. The data that must be agreed on between system entities includes supported roles, identifiers, supported profiles, URLs, certificates and keys.
- Encryption - SAML V2.0 permits attribute statements, name identifiers, or entire assertions to be encrypted. This feature ensures that end-to-end confidentiality of these elements may be supported as needed.
- Attribute profiles - Attribute profiles simplify the configuration and deployment of systems that exchange attribute data. The attribute profiles include:
    - Basic attribute profile: supports string attribute names and attribute values drawn from XML schema primitive type definitions.
    - X.500/LDAP attribute profile: supports canonical X.500/LDAP attribute names and values.
    - UUID Attribute Profile: supports use of UUIDs as attribute names.
    - XACML Attribute Profile: defines formats suitable for processing by XACML.

- Session management - The single logout protocol in SAML V2.0 provides a protocol by which all sessions provided by a particular session authority can be near-simultaneously terminated. As an example, if a user, after authenticating at an identity provider, achieved single sign-on to multiple service providers, they could be automatically logged out of all of those service providers at the request of the identity provider.
- Devices - SAML V2.0 introduces new support for the mobile world, addressing both the challenges introduced by device and bandwidth constraints and the opportunities made possible by emerging smart or active devices.
- Privacy mechanisms - SAML V2.0 includes mechanisms that allow providers to communicate privacy policy and settings. For instance, SAML makes it possible to obtain and express a principal's consent to some operation being performed.
- Identity provider discovery - In deployments having more than one identity provider, service providers need a means to discover which identity provider(s) a principal uses. The identity provider discovery profile relies on a cookie written in a common domain between identity and service providers.

The Benefits of SAML V2.0

Why is InCommon pushing for broad SAML V2.0 support across the Federation? Let’s imagine for the moment that 100% of InCommon IdPs and SPs supported SAML V2.0. Then all of the following would become possible:

- IdPs would encrypt all issued assertions, guaranteeing end-to-end confidentiality and relying party authenticity.

- Because of the enhanced security characteristics associated with encrypted assertions, IdPs would simply push attributes in all cases. No attribute query or artifact resolution would be necessary. No SOAP or back-channel SSL/TLS exchanges would be required.

- With the need for back-channel exchanges all but eliminated, SAML Web Browser SSO would become much easier to deploy. The promise of significantly reduced administrative overhead would induce smaller organizations with limited resources to join the Federation, which would increase the penetration of InCommon throughout the education community.

- SPs could safely choose to deploy SAML V2.0 protocols only, which widens the range of SAML software options available to SP operators.

- A standard approach to SP-initiated Web Browser SSO, along with a rich authentication request protocol, would increase the communication bandwidth between SPs and IdPs, and enable use cases previously found to be ill-suited to federation.

- Support for non-browser SSO would increase the reach of SAML, giving users access to technologies and services previously unavailable via ordinary web browsers.

- A sophisticated framework for defining and transmitting authentication context from the IdP to the SP would enable a framework based on so-called *levels of assurance*. This capability is a prerequisite for the InCommon Identity Assurance Program and the high-valued applications and services it envisions.

The following is a more detailed, technical list of some of the more important advantages of SAML V2.0:

- SAML V2.0 standardizes SP-initiated Web Browser SSO
    - SP-initiated SAML V1.1 Web Browser SSO is based on the proprietary Shibboleth 1.x `AuthnRequest` protocol
- SAML V2.0 provides a rich authentication request protocol (SAML V2.0 `AuthnRequest`)
    - SAML V1.1 doesn’t even have an authentication request protocol
    - InCommon relies on the Shibboleth 1.x `AuthnRequest` protocol (which is functionally limited and nonstandard)
- SAML V2.0 leverages indexed `<md:AssertionConsumerService>` endpoints in metadata
    - these endpoints may be referenced in a `<samlp:AuthnRequest>` message
- SAML V2.0 supports multiple `<md:ArtifactResolutionService>` endpoints in metadata
    - these endpoints are not supported at all by SAML V1.1
- SAML V2.0 leverages multiple `<md:AttributeConsumingService>` elements in metadata
    - these endpoints may be referenced in a `<samlp:AuthnRequest>` message
    - SAML V1.1 supports just one `<md:AttributeConsumingService>` element
- SAML V2.0 provides *many choices* with respect to SAML binding
- SAML V2.0 supports message-level encryption (i.e., XML Encryption)
    - SAML V1.1 doesn’t support XML Encryption at all

- SAML V2.0 provides a standard transient name identifier
  - SAML V1.1 doesn't define a transient name identifier
  - InCommon relies on the proprietary `urn:mace:shibboleth:1.0:nameIdentifier` transient name identifier format
- SAML V2.0 introduces persistent name identifiers
  - these identifiers are compatible with the `eduPersonTargetedID` attribute
- SAML V2.0 provides message-level support for IdP Proxies
- SAML V2.0 provides extensive support for authentication context
  - authentication context is required for participation in the InCommon Identity Assurance Program
- SAML V2.0 defines a non-browser SSO profile (i.e., SAML V2.0 Enhanced Client or Proxy profile)

The OASIS SAML Technical Committee has published a comprehensive list of differences between SAML V2.0 and SAML V1.1 as well.

Taken from: SAML V2.0 Executive Overview (12 April 2005, published by OASIS)