



Fact-Sheet SAML 2.0 (Technical Overview)

Context

- Authentication, Attributes, Authorization
- SAML standard defines an XML-based framework for describing/exchanging security information

Description

- Security Assertion Markup Language (SAML), OASIS standard March 2005
- OASIS Security Services TC
- There is a good technical overview document that is not part of the standard set of specifications
- SAML defines syntax and processing semantics of assertions about a subject by a system entity
- Security information is expressed as portable SAML assertions
- Applications that work across security domain boundaries can trust SAML assertions
- A subject could be a human but could also be some other kind of entity (company or computer)
- An example: user John Doe has email john.doe@xyz.de and he was authenticated into this system using a password mechanism” – a service provider uses that information to grant Joe access
- Multi-domain web single sign-on is the most important use case for which SAML is used
- Another use case is federated identity: share security and identity information about users
- The process of associating a federated identifier with the local identity at a partner where the federated identity will be used is often called **account linking**
- SAML is designed to be highly flexible, extensibility points in XML schemas, guidelines for custom-designing new bindings and profiles to ensure maximum interoperability
- OpenSAML Java/C++ impl. of SAML spec. in version 1.1/1.0 (<http://www.opensaml.org/>), 2.0 in dev.
- SAML 2.0 represents a significant feature upgrade to SAML 1.1

Set of Specifications:

- Standardized SAML 2.0 is a set of specifications
- **Assertions and Protocols:** syntax&semantics for creating XML-encoded assertions to describe authentication, attribute, and authorization information – also protocol message to carry assertions
- **Bindings:** How assertions and req/res protocol messages can be exchanged between systems using underlying communication protocols and frameworks
- **Profiles:** set of rules for using and restricting SAML's syntax for conveying security information to solve specific problems (e.g. Web Single-sign On exchange without cookies)
- **Metadata:** How a SAML entity can describe its configuration data in a standard way for others (e.g. service endpoint, or key material for verifying signatures)
- **Authentication Context:** Syntax for describing authentication context declarations that describe various authentication mechanisms.
- **Conformance Requirements:** requirements to be SAML conform
- **Security and Privacy Considerations:** describes/analyzes security and privacy properties of SAML
- **Glossary:** defines terms used in SAML specifications
- Others are still evolving
 - Metadata Extension for Query Requestors, Attribute Sharing Profile for X.509 Authentication-based Systems, v1.x Metadata, XPath Attribute Profile, Protocol Extension for Third-Party Requests



SAML use cases and drivers

- SAML defines syntax & rules for requesting, creating, communicating, and using SAML assertions
- Drivers of SAML Adoption:
 - Single Sign-on (SSO): SAML solves the multi-domain SSO (MDSSO) problem by providing a standard vendor-independent grammar and protocol for transferring user information from one server to another independent of the server DNS domains
 - Federated identity: provides a means for partner services to agree on and establish a common shared name id to refer to the user (share information across org. boundaries)
 - Web Services and other industry standards: SAML has defined a profile for how to use SAML's rich assertion constructs within WS-Security security token. That can be used to secure SOAP message exchanges
- SAML system entities can operate in a variety of SAML roles which define the SAML services and protocol messages (e.g. SSO support as identity provider (IdP) or attribute authority role where a SAML entity produces assertions in response to identity attribute queries from an entity acting as an attribute requester)

SAML Architecture

- **Components permit transfer of identity, authentication, attribute, and authorization information between an established trust relationship**
- Core SAML spec. defines structure and content of assertions and protocol messages
- SAML assertions carry statements about a principal that an asserting party claims to be true
- Structure and contents of messages are defined by the SAML-defined protocol XML schema
- To transport SAML protocol messages, bindings are defined in SAML bindings (SOAP, HTTP)
- SAML profiles are defined to satisfy a particular use case, e.g. Web Browser SSO profile
- **Profiles define constraints on the contents of SAML assertions, protocols, and bindings**
- Attribute Profiles (that do not refer to any protocol messages) define how to exchange attribute information using assertions in ways that align with a number of common usage environments (e.g. X500/LDAP directories)
- **Assertions: assert security information in form of statements about a subject, three kinds:**
 - **Authentication, Attribute and Authorization decision statements**
- Protocols: a number of generalized req/res protocols:
 - Authentication Request Protocol, Single Logout Protocol, Assertion Query and Req. Protocol, Artifact Resolution Protocol, Name Identifier Management Protocol, Name Identifier Mapping Protocol,
- Bindings: SAML bindings detail exactly how the various SAML protocol message can be transported
- Profiles: define how the SAML assertions, protocols and bindings are combined and constrained
- SAML itself does not make use of the SOAP header, SAML req/res entirely in body
- "Man in the middle attacks" are discussed in detail in the Security/Privacy Consideration document
- SAML usually base upon pre-existing trust relationships that rely on Public Key Infrastructure (PKI)
- WS-Security (protection of SOAP messages) uses SAML assertions in the token element
- WS-Security with SAML is defined in the SAML Token Profile, typically assertions contain a key used for digitally signing data within the body of the SOAP message
- eXensible Access Control Markup Language (XACML) defines the syntax and semantics or a language for expressing and evaluating access control policies, SAML can be used with XACML (SAML 2.0 profile of XACML 2.0)

Links

- <http://www.oasis-open.org/specs/index.php#samlv2.0>