XACML Domain Model

draft-xtc-use-domain-01 7-Jun-01

This document directly references the "SAML Domain Model – draft-sstc-use-domain-04" by Dave Orchard and Hal Lockhart. The definitions and descriptions contained within this document either serve as changes to or additions on the definitions and descriptions contained within the original document.

See end of this document for "changes from prior version" and "author's notes on this version".

Static Model

The SAML Static Model diagram has been amended to that of Figure 1. The "Security Policies" object has been renamed to the "Authorization Policies" object.

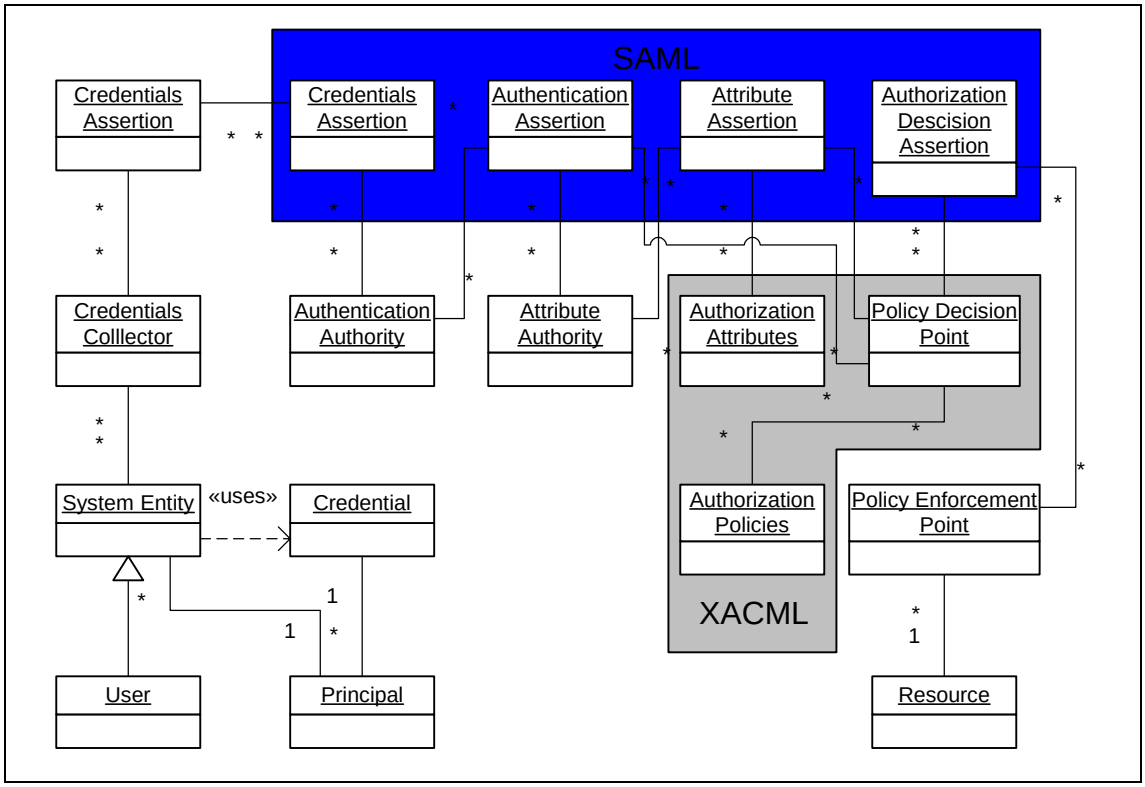

Figure 1 –SAML & XACML Static Model

Issues

- Should the Policy Decision Point be in scope for XACML?

Glossary (abridged):

Authentication: Authentication is the process of confirming an entity's asserted principal identity with a specified, or understood, level of confidence.

The process of verifying a principal identity claimed by or for a system entity.

Synonyms(s): **Sign on.**

Authentication Assertion: Data vouching for the occurrence of an authentication of a principal at a particular time using a particular method of authentication.

Synonym(s): **name assertion.**

Authorization Decision Assertions: Assertions that correspond to the result of an authorization decision. Such assertions must contain the binary result of the decision (permitted/not permitted) and may contain additional "advisory" information that serves to act as an explanation for the decision.

Authorization Policy: An authorization policy is a statement about the terms and conditions under which a given resource can be accessed in a particular way. For example: members of the group "Sonic Death Monkey" are granted "use" privileges on the resource "/usr/bin/guitar".

Policy Decision Point: The place where a decision is arrived at as a result of evaluating the requester's authorization attributes, the requested operation, and the requested resource in light of applicable authorization policy.

Policy Enforcement Point: A component of a resource manager that is responsible for performing authorization queries against the Policy Decision Point and enforcing the resulting Authorization Decision Assertions.

Sign-on: The process of confirming an entity's asserted principal identity with a specified, or understood, level of confidence.

The process of verifying a principal identity claimed by or for a system entity.

Synonyms(s): **Authentication.**

Producer Consumer Model

Figure 2 shows the amended Producer Consumer Diagram for XACML. Notice that the Session Authority and Session Assertions have been removed from this diagram pending completion of the work undertaken by the SAML Sessions Focus Group.

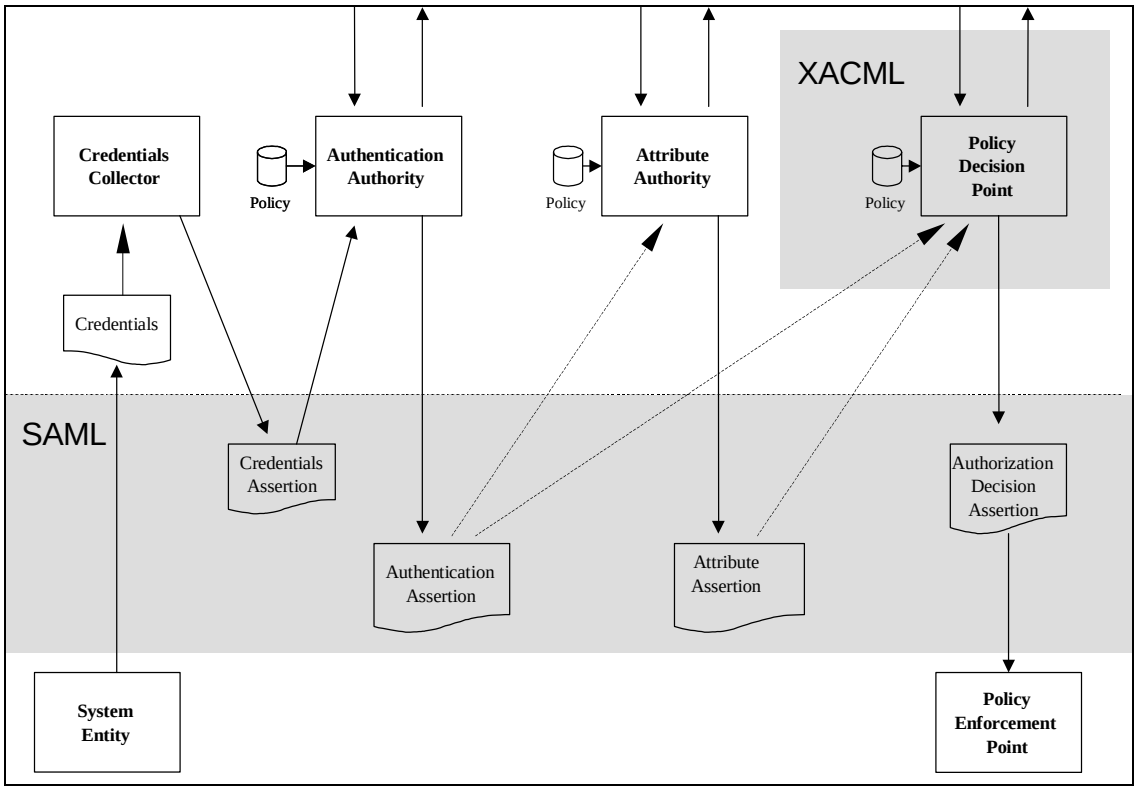

Figure 2 - Producer Consumer Diagram

Changes from Prior Version

- Reworked Figure 1 –SAML & XACML Static Model to delineate those elements that are defined by SAML versus those elements that are defined by XACML. Renamed the “Security Policies” element to “Authorization Policies”.
- Reworded some definitions in the Glossary and removed the links to SAML documents.
- Reworked Figure 2 – Producer Consumer Model to delineate those elements within the scope of XACML. Also removed the Session Authority and Session Assertions pending completion of the work undertaken by the SAML Sessions Focus Group.

Author’s Notes on this Version

- I am disturbed about the fact that Authorization Attributes appear in Figure 1 but don’t appear in Figure 2. Are there attributes who’s schema are likely to closely coupled with the Authorization Policies defined within the security domain? Does the definition of these attributes then fall within the scope of XACML?