Domain Model -- draft-sstc-use-domain-03

Use Case & Requirements Subgroup,
OASIS Security Services Technical Committee (SSTC)
3-Apr-2001

Dave Orchard, Jamcracker
Hal Lockhart, Entegrity

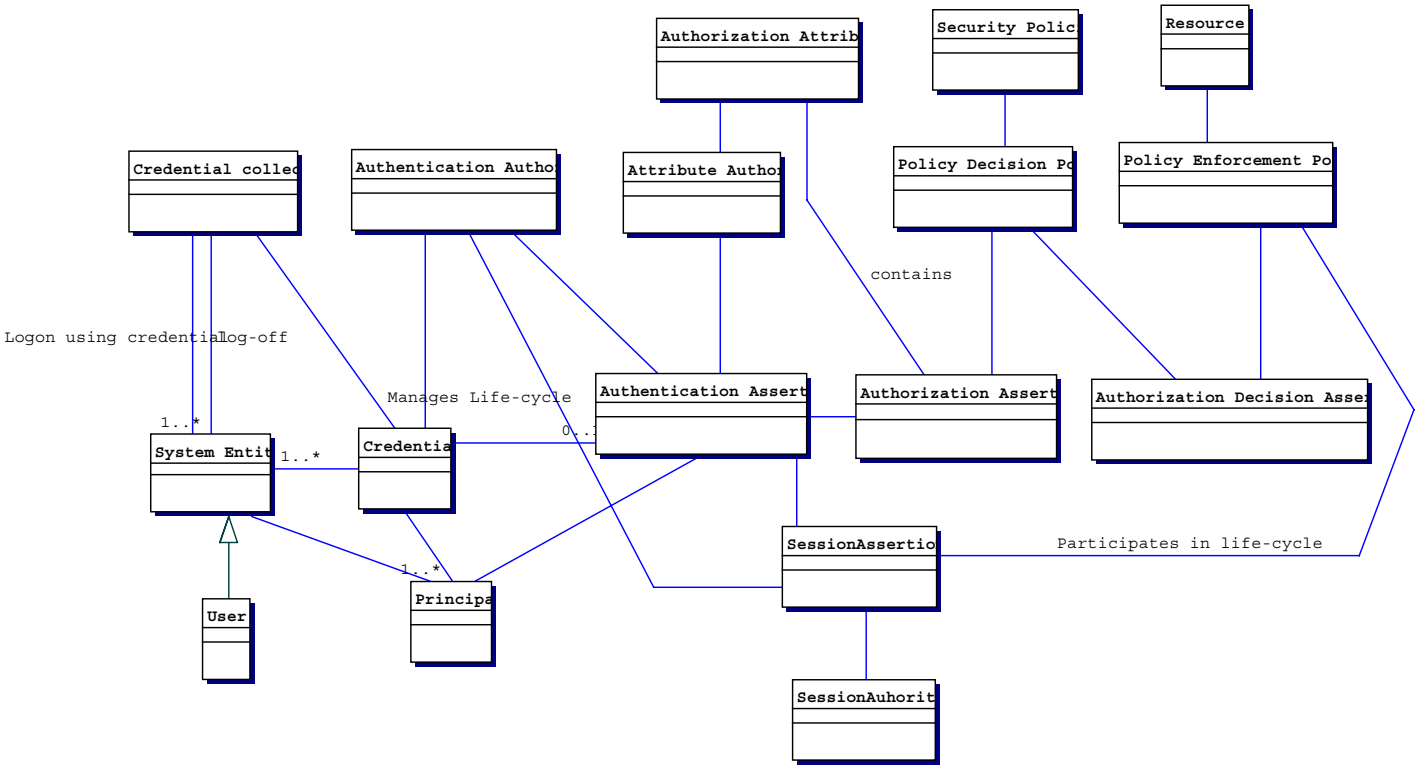
Introduction

This domain model provides a description and categorization of the domain that SAML solves problems in. People, software, data, interactions, and behavior are described in the abstract, without binding the specification to a particular implementation. It provides a standardized or normalized description of concepts for the purposes of further discussion in requirements, use-cases, etc. It covers material out-of-scope for the specification in order to show the context that the specification solves problems in. It does not describe implementation information such as API details, Schema definitions and data representations.

A typical use-case for this document is: "We all agree what we mean by term x and how entity y creates it and entity z consumes it. Is x in scope or out of scope for SAML?". Another use case "We have created an OASIS TC committee on functionality A. A is the standardization of term x that is out of scope for SAML".

In the rational unified process, an artifact we are working on is the logical view, http://www.rational.com/products/whitepapers/350.jsp#RTFToC2.

Static Model



Glossary (abridged):

Notation: Definitions that have been agreed upon by the use case subgroup are denoted(Conf)

Assertion: TBD

Attribute Authority: (Conf) A system entity that produces Attribute assertions, based upon TBD inputs.

Attribute Assertion: An assertion about attributes of a principal.

Authentication – (from glossary with principal added) (Conf) Authentication is the process of confirming an entity's asserted principal identity with a specified, or understood, level of confidence. [7]
The process of verifying a principal identity claimed by or for a system entity. [12]

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.

Authentication Authority: (Conf) A system entity that verifies credentials and produces authentication assertions

Authorization Attributes: (Conf) Attributes about a principal which may be useful in an authorization decision (group, role, title, contract code,...).

Authorization Decision Assertions: (from glossary) In concept an authorization assertion is a statement of policy about a resource, such as:
the user "noodles" is granted "execute" privileges on the resource "/usr/bin/guitar."

Authorization Assertion: A data structure that contains Authentication Assertions and Authorization attributes.

Credential: (Conf) Data that is transferred or presented to establish a claimed principal identity.

Log-on: The process of presenting credentials to an authentication authority for requesting access to a resource

Log-off: The process of informing an authentication authority that previous credentials are no longer valid for a User Session

Policy Decision Point: (from glossary, access control decision) The place where a decision is arrived at as a result of evaluating the requester's identity, the requested operation, and the requested resource in light of applicable security policy. (surprisingly enough, not explicitly defined in [10])

Policy Enforcement Point: (from glossary, access enforcement function) The place that is part of the access path between an initiator and a target on each access control request and enforces the decision made by the Access Decision Function [10].

Principal, or Principle Identity: (Conf) An instantiation of a system entity within the security domain.

Resource: (from glossary) Data contained in an information system (e.g. in the form of files, info in memory, etc); or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment. (definition from [1])

Security Domain: TBD

Security Policies: (from glossary) A set of rules and practices specifying the "who, what, when, why, where, and how" of access to system resources by entities (often, but not always, people).

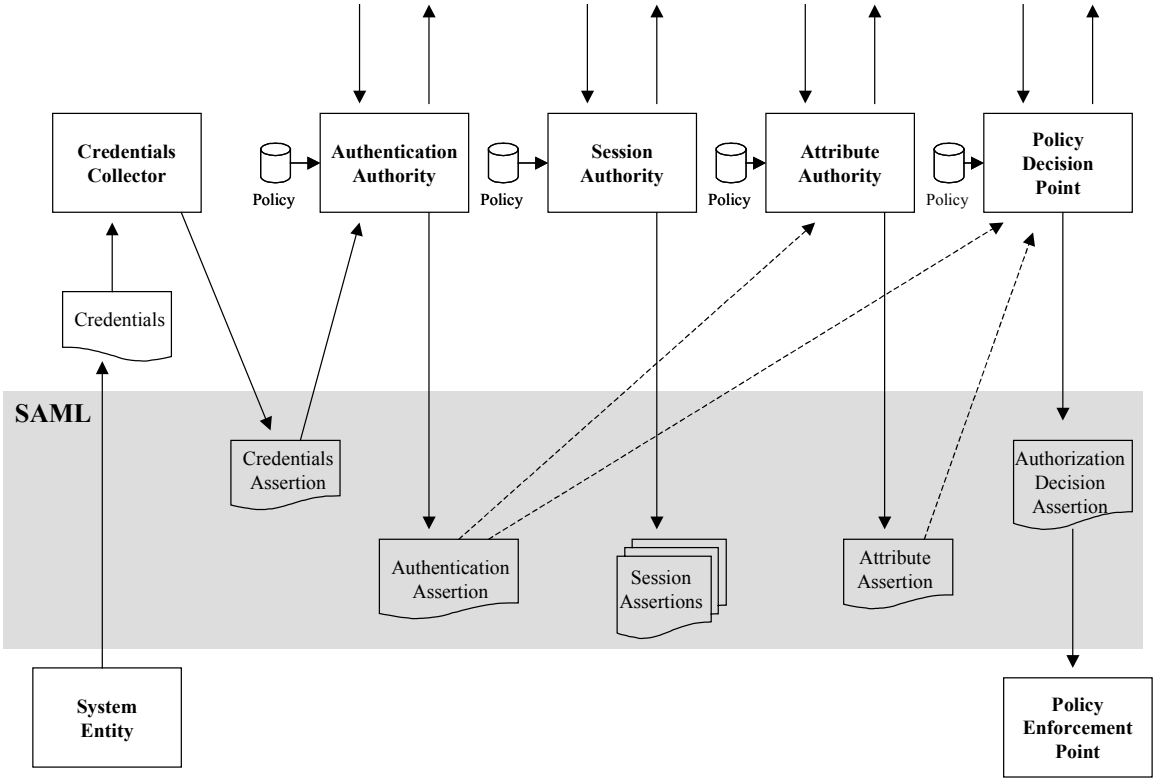
System Entity: (from glossary) (Conf) An active element of a system--e.g., an automated process, a subsystem, a person or group of persons--that incorporates a specific set of capabilities. (definition from [1])

Time Out: A step where an authorization assertion is deemed no longer viable. Subsequent resource requests from a user must proceed with log on.

User: (Conf) A human individual that makes use of resources for application purposes

User Session: A container for the authentication and attribute assertions that apply to a given system entity through the principals incarnated by that entity. The purpose is to maintain the relationship of the assertions to the initiating entity.

Producer Consumer model



This diagram provides a view of the elements of the SAML problem space that is focused on the architectural entities and their inputs and outputs. Its main purpose is to achieve a sufficient commonality of understanding the meanings of the various terms used to allow productive discussion. The names have been chosen either to be consistent with standard usage in the field or suggestive of their purpose or action, in many cases their exact nature or contents are not fully agreed upon. Although the diagram is intended to be neutral on the SAML design, the choice of which elements to include and which to leave out anticipates likely elements of the design.

This diagram should **not** be interpreted as describe message flows or a single processing flow. It merely attempts to describe which entities are capable of producing certain outputs and which entities may make use of certain inputs. For example, all of the following are consistent with this diagram:

- A PDP collects various assertions from their sources in order to make a policy decision
- An Attribute Assertion is returned to the System Entity that initiated the interaction (lower left) who presents it as required

- A PDP makes a decision without the use of any assertions

All of the entities shown may be a part of distinct security domains, or some of them may be in the same domain. Typically there will only be two or three security domains involved. Common groupings include:

- Combined Authentication Authority and Attribute Authority
- Combined PEP and PDP
- All combined except for PEP

Many of the components can have multiple instances. For example, there can be multiple Attribute Authorities or multiple PDPs. This may introduce relationships not shown in the diagram, for example, a PDP might provide assertions to another PDP.

There is an asymmetry between input and output. The outputs that are standardized have the names shown, by definition. The entities may or may not use the inputs identified for any particular action. This is represented by the use of solid and dashed lines respectively.

The entities that have an associated policy store, are assumed to use that policy to modulate the outputs they produce. This policy store is assumed to be non-volatile and capable of being administered in some way. The unlabeled arrows at the top represent other inputs and outputs, not specified by SAML. For inputs these fall into two categories: 1) inputs which have the same semantics as SAML defined Assertions, but are in unspecified format and 2) items which are not specified by SAML at all. An example of #1 is an X.509 Attribute Certificate. An example of #2 is the current date and time.

The diagram anticipates the design of SAML by identifying only the security assertions that could be output by these entities. SAML will also have protocol messages to send and receive these assertions and will make use of existing communications protocols to transmit these assertions.

The central gray box labeled SAML indicates which assertions **may be** specified by SAML. In particular, the inclusion of Credentials Assertions and Sessions Assertions has not been settled.
The definitions of these items can be found elsewhere.

The following comments cover points that may not be completely evident.

The System Entity in the diagram is the one requesting some action that will ultimately be permitted or denied. As a preliminary step it may provide credentials to authenticate itself.
The Credentials are not merely limited to a password, but might involve a sequence of messages exchanges, for example in a Public Key authentication protocol.

The Credentials Collector is an entity that can front-end the authentication process and pass to the Authentication Authority the information necessary for it to authenticate the System Entity. This is similar to the functionality provided by the RADIUS protocol.

The exact nature of Session Assertions has not been determined at this point. Therefore it is unknown what entities might consume them.

The Authorization Decision Assertion might simply provide a yes/no response, or it might provide specific information about why access is denied, or it might provide statements of policy.

The Policy Enforcement Point is defined to have no policy, but to act directly on the contents of the Authorization Decision Assertion.