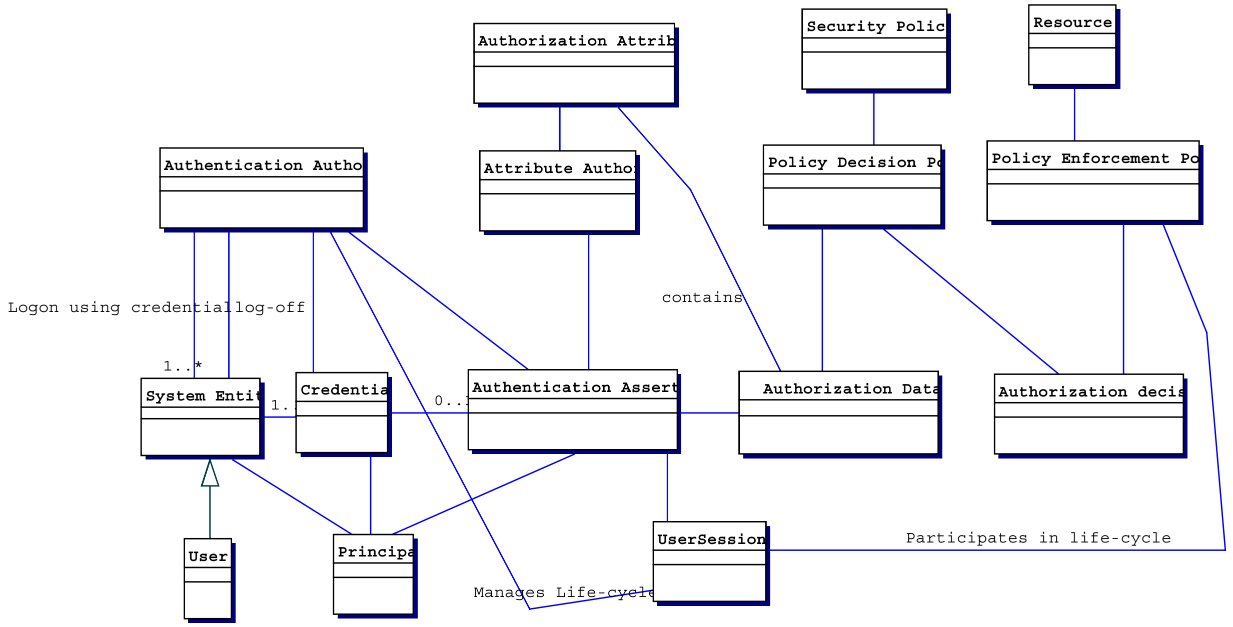
Introduction

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.

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 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."
Issue: Should this be Authorization Decision

Authorization Data: 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.