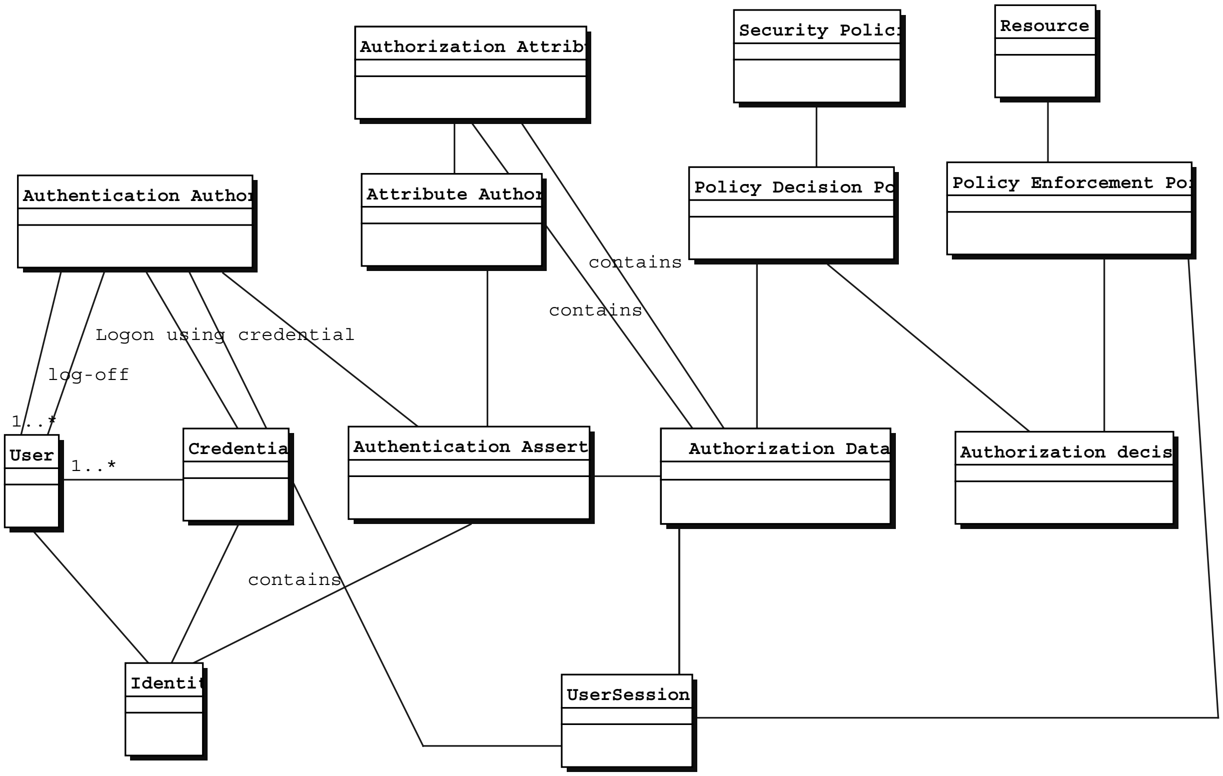
# Introduction

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):*

**Attribute Authority ?**

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

**Authentication Assertion:** (from glossary) "Data that is transferred to establish the claimed identity of an entity." [9]

**Authorization Attributes -** 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 –** (from glossary) Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity. (See also: assertion, authentication information, capability, ticket.) [1]
"Data that is transferred to establish the claimed identity of an entity." [9]

**Credential**: (alternate definition) A data structure that contains at least one attribute (e.g. a name or entitlement) of a Principal. It may, in addition, contain information (such as a password digest or public key) by which the Principal can demonstrate that it is the subject of the credential. (Note: the current Glossary defines "credential" in terms of what it "is used for", not what it "is". So, I think the definition presented here is more useful for our purposes).
Issue: which of the definitions shall be chosen?

**Identity:** (from glossary) A representation (e.g. a string) uniquely mapped to an entity (e.g. an end user, an administrator, or some process, or some network device).

**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

**Name Assertion?**

**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?** Is a Principal a User?

**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 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).

**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:** (from glossary) An entity, usually a human individual, that makes use of resources for application purposes

**User Session:** A construct produced by an authentication authority that defines the life-time of an authorization assertion