MappingXacmlSignetTerms

Mapping XACML and Signet Terms

Summary: *This page compares key terms used in the XACML Domain model and the Signet project. The material within is intended to be used as a discussion starter for the Signet-dev/MACE-paccman work group to establish common language/terminology around Access Managment discussions.*

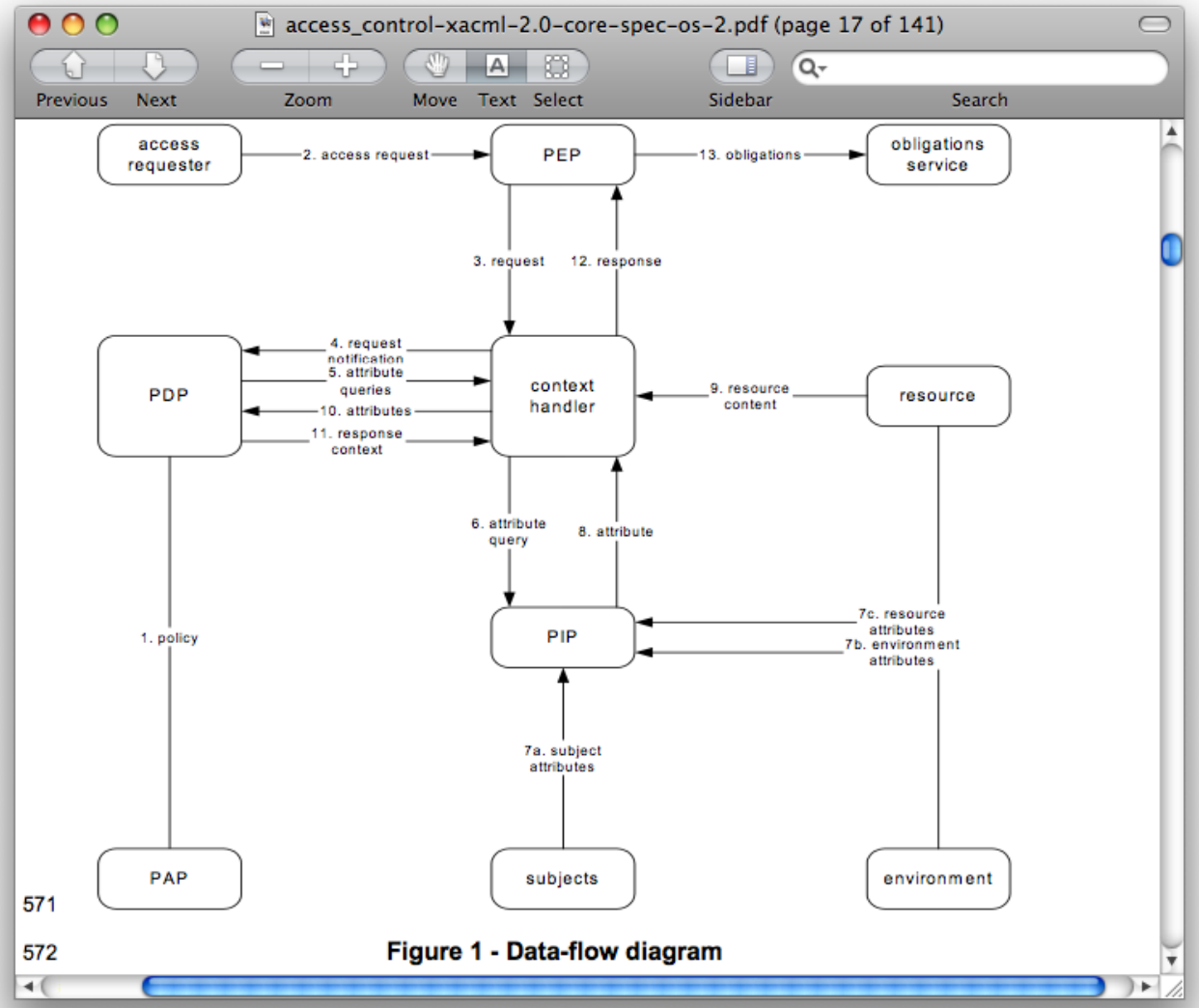
As of May 2012, this page is also being used as helpful XACML reference for the project of modeling selected use cases using XACML terms.

Table of Content

- Table of Content
- Key XACML Concepts
- Observations
- Term Mapping
- References

Key XACML Concepts

- **Policy administration point (PAP)** - The system entity that creates a ***policy*** or ***policy set***.
- **Policy decision point (PDP)** - The system entity that evaluates ***applicable policy*** and renders an ***authorization decision***.
- **Policy information point (PIP)** - The system entity that acts as a source of ***attribute*** values.
- **Policy enforcement point (PEP)** - The system entity that performs ***access control***, by making ***decision requests*** and enforcing ***authorization decisions***.
- **Context handler** - The system entity that converts ***decision requests*** in the native request format to the XACML canonical form and converts ***aut horization decisions*** in the XACML canonical form to the native response format.
- **Action** - An operation on a ***resource***.
- **Access** - Performing an ***action***.



(XACML Data Flow Model diagram, p. 17, **[XACML]**.)

Observations

- XACML defines a more complete model of access control than covered by Internet2 tools. For example, XACML specifies the relationship and the messaging syntax between PEP and PDP. There is no direct equivalent in the Internet2 model.
- Signet appears to be an implementation of a ***PAP*** per XACML's domain model.
- Shibboleth/LDAP directory can be interpreted as a PIP or a PDP, depending on the context in which it is used.
- Signet model suggests that PDP and PEP responsibilities are left to the application. Alternatively, one might turn Shibboleth into a PDP by asserting authorization decisions via eduPersonEntitlement. Either way, authorization decisions are always *enforced* within the application.

Term Mapping

XACML	Signet	Comment

Subject An actor whose attributes may be reference by a predicate. The entity to which an access policy applies	**Subject** A person or a group. **Grantee** The subject who is receiving privileges.	In XACML, the concept of "Group A can do x." is expressed as "An individual who is a member of group A can do x", "An individual with role A can do x." "Subject", in this context, is really the combination of an individual plus all of his group/role membership and other attributes. This aligns more closely with the concept of "Principal", or "Security Principal" in security models in frameworks such as Microsoft .NET.
Resource Data, service or system component	**Resource** Data, service, or system component	There isn't an explicit definition of "resource" in Signet documentation, but the term appears to be used in a way consistent with XACML's definition.
Action An operation on a resource	**Action**	There isn't an explicit definition of "resource" in Signet documentation, but the term appears to be used in a way consistent with XACML's definition.
Condition **Environment**	**Limit Condition** **Prerequesite**	
Rule A target, an effect and a condition. **Access** Performing an Action	**Permission** **Entitlement**	In XACML, a target is a set of resource, subject and action. Roughly translated, a rule is a statment of "<subject> is <Permitted/Denied> access to perform <action> on <resource> when <condition> is met". Note: a condition here may be "actor is a member of group X". "Permission" in Signet appears to state: "<subject> can perform <action> on <resource> when <limit> is satisfied". However, permission may also be better mapped to "access" In XACML terms.
Authorization decision	**Entitlement**	In XACML, an authorization decision is the resulting return value of evaluating a set of applicable policies. It basically is "Permit", "Deny", "Inderterminate", or "NotApplicable". If entitlement is used in the context of "asserting an entitlement value means the person is permitted to access a pre-determined, implied set of resources, then the presence of absence of particular entitlement value could be interpreted as an authorization decision.
Policy, Policy Set	**Privileges**	They are not equivalent, but close...
?	**Function**	

References

[XACML] XACML 2.0 Core Specification
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[Signet] Signet Concepts, Glossary, Features
https://wiki.internet2.edu/confluence/x/HRI

[Powerpoint] "Managing Roles and Privileges with Grouper and Signet Middleware"
http://www.internet2.edu/presentations/spring06/20060426-groupersignet-mcrae.ppt

[Diagram] "Integration Technologies for Grouper & Signet" Diagram
https://wiki.internet2.edu/confluence/download/attachments/3760/integration-02-sml.jpg