Introduction to XACML

What is XACML?

XACML "eXtensible Access Control Markup Language" is an open standard XML based language. The standard defines a declarative fine-grained, attribute-based access control policy language, an architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies. (*)

XACML policy language: is used to describe general access control requirements

XACML request/response protocol: used to query a decisioning engine that evaluates real-world access requests against existing XACML policies.

XACML reference architecture: provides a standard for the deployment of necessary software modules to achieve efficient enforcement of XACML policies.

Terminology

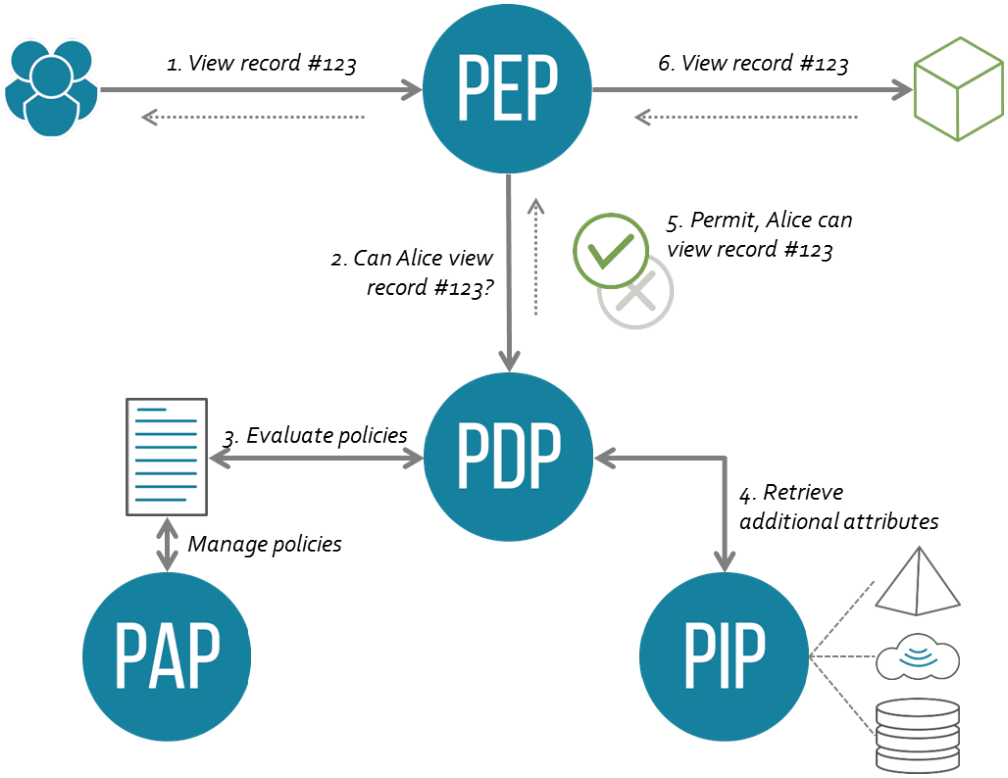
- **PAP - Policy Administration**: Point Point which manages access authorization policies.
- **PDP - Policy Decision Point**: Point which evaluates access requests against authorization policies before issuing access decisions.
- **PEP - Policy Enforcement Point**: Point which intercepts the user's access request to a resource, makes a decision request to the PDP to obtain the access decision
- **PIP - Policy Information Point**: It is the system entity that acts as the source of attribute values. It provides additional information about the attributes needed by the **PDP (Policy Decision Point)** to make authorization decisions.
- **PRP - Policy Retrieval Point**: Point where the XACML access authorization policies are stored, typically a database or the filesystem.

(*) Wikipedia definition

Flow

1. A user sends a request which is intercepted by the Policy Enforcement Point (PEP).

2. The PEP converts the request into a XACML authorization request and forwards the authorization request to the Policy Decision Point (PDP).
3. The PDP evaluates the authorization request against the policies it is configured with. The policies are. acquired via the Policy Retrieval Point (PRP) and managed by the Policy Administration Point (PAP).
4. If needed it also retrieves attribute values from underlying Policy Information Points (PIP).
5. The PDP reaches a decision (Permit / Deny / NotApplicable / Indeterminate) and returns it to the PEP.



(*) Wikipedia definition

In Soffid, PAP and PIP are implemented on the Console.

Soffid XACML

Using the XACML addon it is possible to add access controls XACML standard to the Soffid console. In this case, Soffid can be able to add more complex and restricted rules to the authorizations.

(*) https://en.wikipedia.org/wiki/XACML

(**) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#XACML20

https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

---

Revision #15
Created 16 July 2021 14:22:15
Updated 14 March 2025 09:15:34