Proposal Draft for XACML Context

April 23, 2002

Author: Michiharu Kudo

This proposal introduces an *XACML Context* that defines input parameters to XACML policy evaluation engine. A primary purpose of the XACML Context is to facilitate the attribute expression that refers to input parameters of the XACML.

1. Issues

When XACML policy evaluation processor tries to retrieve values specified in SAML Request, it potentially causes the following problems:

- A policy writer needs to add a couple of information that may not be included in SAML Request, e.g. distinction between subject attribute and resource attribute

- XACML policy specification greatly depends on SAML Request syntax and the semantics that may be updated from time to time.

- Since several assertion specification format/syntax/semantics have been proposed/deployed, SAML dependent XACML policy specification may reduce the applicability of XACML policy specification.

2. XACML Context

We introduce the notion of *XACML Context* that functions as an intermediate assertion-neutral input data structure. XACML Context is represented by an XML document (logically it is not necessarily a physical XML instance but hypothetical XML document) that contains enough information for XACML processor such as subject attributes (e.g. role of the requesting principal), resource attributes (e.g. size of resource), and miscellaneous attributes (e.g. current time). While we assume that all the input to XACML Context is retrieved from the corresponding SAML Request, there is a case where the PDP supplies a set of attribute type-value pairs for subjects and resources. It depends on configuration of PDP.

2.1 Merits

- XACML Policy specification becomes simpler with respects to attribute reference and its expression.

- XPath computation is done only once when the transformation from original access request to XACML Context is performed.

- XACML processor does not have to compute XPath expression on target XML resource that might cause performance bottleneck particularly when the target XML is huge.

- When target resource is XML, XACML policy does not have to be aware the difference between remote XML instance (referred by URI) and local XML instance embedded in original access request.

2.2 Proposal

1. XACML policyStatement (and/or policySetStatement) specifies optional <transforms> element that defines the syntax and the semantics of the XACML Context.

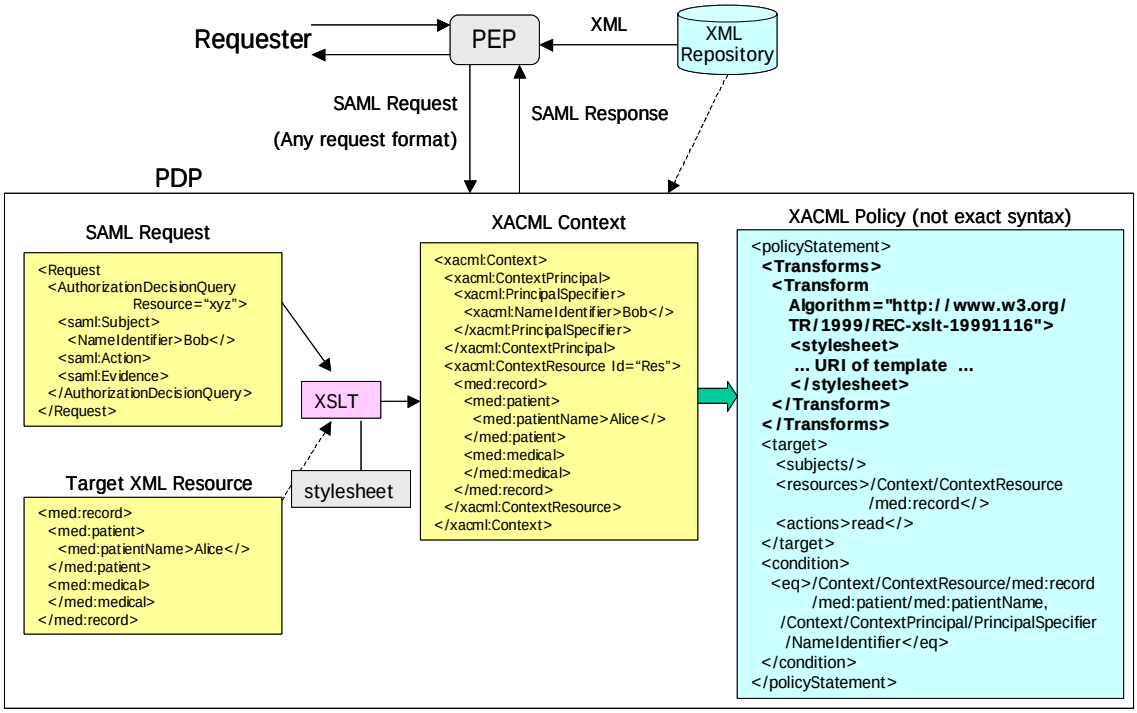
2. <transforms> is described using XSLT syntax.

3. When <transforms> element is specified in <policyStatement>, PDP performs a set of transformations against the SAML Request (if access request is represented in SAML) and the requested XML target resource (if target is XML resource)

4. Once the transformation is performed, input to the XACML processor including access request and relevant information is specified as a potentially simple XML document which element name is easily referred by simple XPath expressions (e.g. /context/subject/NameIdentifier) in both <target> section and <condition> section.

5. Through the face-to-face discussion by TC members, we decided to define an XML schema for XACML Context.

The following figure shows a data-flow of XACML Context-based Architecture.


Requester
PEP
XML
XML Repository
SAML Request
(Any request format)
SAML Response
PDP
SAML Request
<Request
<AuthorizationDecisionQuery
Resource="xyz">
<saml:Subject>
<NameIdentifier>Bob</>
<saml:Action>
<saml:Evidence>
</AuthorizationDecisionQuery>
</Request>
XSLT
Target XML Resource
<med:record>
<med:patient>
<med:patientName>Alice</>
</med:patient>
<med:medical>
</med:medical>
</med:record>
stylesheet
XACML Context
<xacml:Context>
<xacml:ContextPrincipal>
<xacml:PrincipalSpecifier>
<xacml:NameIdentifier>Bob</>
</xacml:PrincipalSpecifier>
</xacml:ContextPrincipal>
<xacml:ContextResource Id="Res">
<med:record>
<med:patient>
<med:patientName>Alice</>
</med:patient>
<med:medical>
</med:medical>
</med:record>
</xacml:ContextResource>
</xacml:Context>
XACML Policy (not exact syntax)
<policyStatement>
<Transforms>
<Transform
Algorithm="http://www.w3.org/
TR/1999/REC-xslt-19991116">
<stylesheet>
... URI of template ...
</stylesheet>
</Transform>
</Transforms>
<target>
<subjects/>
<resources>/Context/ContextResource
/med:record</>
<actions>read</>
</target>
<condition>
<eq>/Context/ContextResource/med:record
/med:patient/med:patientName,
/Context/ContextPrincipal/PrincipalSpecifier
/NameIdentifier</eq>
</condition>
</policyStatement>