XACML – Summary of Use Cases

Aug 7, 2001

V 0.11

Editor: Suresh Damodaran

Status of this Document

This document is created to present to XACML a summary of use cases. The contents of this document are provided by various use case submitters including the author.

1 Overview

The following use cases are considered.

1. Healthcare (HL7) (Fred Moses)
2. DRM (Thomas)
3. ebXML (registry) use case (Suresh)
4. Financial Regulatory use cases (Simon)
5. Online server use cases (Hal)
6. Access control use cases (Michiharu)
7. Pierangela's use case
8. Federal Interagency Records Council use case (Simon)

2 Use Cases

2.1 HL7 Use cases

1) Patient (Ms AXS) with abusive x-spouse who is also insurance subscriber requests restricted access to address and phone portion of record header.
    a) Ms AXS'record document is transmitted to physical therapy facility following diagnosis of acute tendonitis; restriction to address and phone information accompanies transmitted document.
    b) Information regarding services and associated charges are transmitted to outside claims payor. Address and phone restriction follows the information being transmitted, and address and phone of patient are withheld from the EOB.
2) Patient grants entitlement access to psychiatric notes only to primary care doctor. Primary care doctor grants access to patient record to a covering doctor or practice, with entitlement restriction following the transmitted documents so that covering doctor/practice have no access to psych notes.

3) Patient restricts entitlement to HIV screen results, and at a later date presents in the ER with severe trauma; entitlement restrictions are overridden.
4) Patient is him or herself a caregiver in the medical system in which he or she is being treated. Patient requests entitlement restriction of entire record, granting access solely to primary care doctor. Access to record of services and associated charges are granted to billing staff if billing is done in house.

2.2 DRM Use cases [DRMUC1]

2.2.1 Provider-To-Distributor Rights Conferral

Consumer challenges the distributor to prove its distribution rights to sell a specific content.

2.2.2 Distributor-To-Consumer Usage-Rights Conferral

2.2.3 Consumer-To-Consumer Usage-Rights Conferral

2.3 EbXML Registry Use cases [ebUC1]

2.3.1 Restricting Read-Only Access

A Submitting Organization (SO) submits a RegistryObject to a Registry. SO also submits an AccessControlPolicy associated with a RegistryObject. This AccessControlPolicy allows only selected partners of SO to have read-only access to the RegistryObject. All objects in the registry have a unique id specified by *Universally Unique Identifier (UUID)* and must conform to the format of a URN that specifies a DCE 128 bit UUID as specified in UUID [UUDI].The partners (Principal) may be specified in the AccessControlPolicy using Identity, Role, or Group of Users in Organizations. It is assumed that the partner information is available through Organization for all authenticated Users. Partner may also be a RegistryGuest.

2.3.2 Write-Access Beyond the Owner

A Submitting Organization (SO) submits a RegistryObject to a Registry. SO also submits an AccessControlPolicy associated with a RegistryObject. This AccessControlPolicy allows write (modify/deprecate/delete) access to some of the partners of SO. All objects in the registry have a unique id specified by *Universally Unique Identifier (UUID)* and must conform to the format of a URN that specifies a DCE 128 bit UUID as specified in UUID [UUDI].The

partners (Principals) may be specified in the AccessControlPolicy using Identity, Role, or Group. It is assumed that the partner information is available as Organization (*is a* RegistryEntry) for all authenticated Users.

2.3.3 Administrative Use case

The SO submits an administrative access control policy for the administration of access control policies submitted by that SO.

2.4 Financial Regulatory Use cases [FRUC]

2.4.1 Customer Data Use Or Disclosure

An employee in a financial services company wishes to use customer data and does not know the constraints on the use of the data.

2.4.2 Cross-Marketing

A telemarketing employee in the insurance affiliate of a consumer bank receives a request to cross-market an insurance product to a consumer banking customer based on the age of the customer and household information derived from other accounts held by parties at the same address.

2.4.3 Service Delivery

A member of the IT department receives a request to deliver a data extract to Statement Services Corporation. Sensitive customer data, e.g. account numbers and balances are encrypted at the database level.

2.5 Online server Use cases [OSUC]

This use case is intended to cover a variety of online server application environments, such as HTTP; Java Applications, including Servlet, Java Server Pages and J2EE; and CORBA. It could also apply to emerging environments, such as XML Protocol. In general, an online server controls some resources and acts as a Policy Enforcement Point (PEP), controlling whether requests should be allowed or not. A Policy Enforcement Point (PDP) evaluates the policies that apply. The PDP may be located within the server or accessed remotely.

2.6 Access Control on XML Resources Use cases [ACU1]

2.6.1 System Configuration

This is a scenario for an element-wise access control in retrieving a XML resource e.g. a system configuration file stored in the server:

```
<?xml version="1.0"?>
<configuration>
<keyStore>key.db</keyStore>
<docRoot>/</docRoot>
<qos_policy>qos.xml</qos_policy>
<security_policy>policy.xml</security_policy>
</configuration>
```

It is often the case that some elements of the configuration contents are read only by a specific user (e.g. a security administrator.)

2.6.2 Element-wise Access Control in Updating XML

This is similar to the previous scenario but the access mode is "write". An element-wise update control is necessary if one XML resource contains elements that are classified in different security levels.

2.6.3 Online Catalogue

This is a typical online shopping application for cyber marketplaces. XML is used to store online catalog data that contains items for sell. There are two classes for buyers: normal members and premium members. The catalog includes all available items, including some that are available only to premium members. Selling information is labeled as "normal", "premium", or "all". The access control policy says that the normal members cannot read any information for premium members, and the premium members cannot read any information for normal members. You will see how the XML access control can be applied to the practical applications through this example.

2.6.4 Paper Reviewing

This application simulates a typical review process for academic papers. This example illustrates how the XML access control is applied to applications that need information sharing and/or updating among multiple participants who play different roles. The review process can be described as follows:

1. Authors submit their papers to the submission server. A chairperson assigns one or more reviewers to each submitted paper.
2. The reviewers read the assigned paper and evaluate it.
3. The program committee members read the reviewers' evaluations and decide whether or not each paper should be accepted.
4. The chairperson decides on the list of accepted papers.
5. The authors receive notifications of acceptance or rejection.

2.6.5 Medical Record

This application illustrates how the XML access control can be applied to the domains that require more complicated access control specifications such as a context dependent access control. This application is taken from the medical domain. A medical record stores medical history such as diagnosis results and the chemotherapy history for a patient. The advantages of representing medical records in XML format would be a platform-independent plain-text format and the features of the digital signature. It is often said that patients want to be properly informed by the doctor in charge so they can give their informed consent to treatment. One way to achieve this goal is for the doctor and the patient to sign a document that confirms that the patient was well informed and consented to the procedure. Since XML provides a mechanism to store the digital signature inside the document, XML is an appropriate format to represent medical records.

2.6.6 Policy Management

One advantage of using the XML format for specifying access control policies is that the policy language can easily implement the policy management authorization rules. In other words, authorization rules on the authorization policy itself can be defined by meta-rules also described in the same language. Here we take the access control policies of the second example, online catalogue, as a target XML document.

2.6.7 Access Control of Non XML Resources

This scenario illustrates another application scenario. The target XML resource is never displayed or updated in this example, but it is used only for making access decisions.

2.7 Pierangela's use case [ACM1]

2.8 FIRMC Use case [FIRMC]

Received by Simon from Federal Interagency Records Management Council.

1. Every individual controls access to his or her own personal data,
2. Each individual can quickly and easily determine the constraints under which he or she is willing to empower others to access and use his or her data, and
3. Every use of each element of data will be recorded and those records will be maintained for as long as required by law or desired by the individuals whose records are at issue.

3 References

[ACM1] http://sansone.crema.unimi.it/~samarati/Papers/sec01.ps

[ACU1] Access Control on XML Resources, http://lists.oasis-open.org/archives/xacml/200107/msg00023.html

[DRMUC1]DRM Use Cases, http://lists.oasis-open.org/archives/xacml/200107/msg00072.html

[FRUC] Financial Regulatory use cases, http://lists.oasis-open.org/archives/xacml/200108/msg00005.html

[ebUC1] ebXML Registry Use cases, http://lists.oasis-open.org/archives/xacml/200107/msg00022.html

[FIRMC]Federal Interagency Records Management Council, http://lists.oasis-open.org/archives/xacml/200108/msg00006.html

[OSUC] Online Server Use Cases, http://lists.oasis-open.org/archives/xacml/200108/msg00004.html

[UUID] DCE 128 bit Universal Unique Identifier http://www.opengroup.org/onlinepubs/009629399/apdxa.htm#tagcjh_20

http://www.opengroup.org/publications/catalog/c706.htmttp://www.w3.org/TR/REC-xml