XACML – Summary of Use Cases

September 7, 2001
V 0.2
Editor: Suresh Damodaran, Carlisle Adams

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.

1. Overview
The following use cases are included:

1. Healthcare HL7 (Fred Moses)
2. DRM (Thomas Hardjono, David Parrott)
3. ebXML Registry (Suresh Damodaran)
4. Financial Regulatory (Simon Blackwell)
5. Online server (Hal Lockhart)
6. Access control on XML Resources (Michiharu Kudo)
7. Access control model for data archives (Pierangela Samaratti)
8. Federal Interagency Records Council (Simon Blackwell)
9. Workflow (Carlisle Adams)
10. Microsoft.NET Stack Walk (Carlisle Adams)
11. Policy Analysis (Key Yagen)
12. WebDAV (Bill Parducci)

2. Use Cases

2.1 HL7 Use cases

1) Patient (Ms AXS) with abusive ex-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

Comment: Page: 1
End user can set some aspects of policy.

Comment: Page: 1
Policy must be mobile (e.g., accompany data, or be sent by an alternate route).

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.

Comment: Page: 2
Delegation of privilege required.

3) Patient restricts entitlement to HIV screen results, and at a later date presents in the ER with severe trauma; entitlement restrictions are overridden.

Comment: Page: 2
Policy can be overridden (or, preferably, emergency access is part of policy), with proper audit.

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.

Comment: Page: 2
Location-based policy rules required.

In all cases, there may be a requirement to audit the decision that was made for a future record of what was done and when (and perhaps why).

2.2 DRM Use cases [DRMUC1, DRMUC2]

2.2.1 Provider-To-Distributor Rights Conferral [DRMUC1]

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

Comment: Page: 2
This may simply be a SAML attribute assertion, but ***proof*** may require consumer access to actual policy (i.e., rendering of policy to GUI, as well as verification that policy is valid).

2.2.2 Distributor-To-Consumer Usage-Rights Conferral [DRMUC1]

Comment: Page: 2
Possibly delegation, but possibly just provider (consumer trust anchor) being able to specify that distributor can assign this authority.

2.2.3 Consumer-To-Consumer Usage-Rights Conferral [DRMUC1]

Comment: Page: 2
Definitely delegation (with associated restrictions/constraints).

*(**Editor's note:** 2.2.1 - 2.2.3 seem more like SAML attribute assertion use cases than XACML use cases.)*

2.2.4 Reuters' requirements for rights data dictionary and rights expression language [DRMUC2]

(See document for extensive collection of use cases.)

Comment: Page: 2
Document also has extensive collection of requirements that are relevant to XACML, particularly pp.17-54).

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.

Comment: Page: 3
Policy language (or, preferably, the evaluation system [PRP and/or PDP]) must understand and accommodate a variety of actions on resources.

Comment: Page: 3
Policy language must accommodate a variety of ways of identifying resources.

Comment: Page: 3
Policy language must accommodate a variety of ways of identifying the owner of a privilege.

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.

Comment: Page: 3
Again, a variety of actions (that may be specific to an environment, context, or vertical, such as "deprecate").

Comment: Page: 3
Privilege information may not accompany a request (i.e., must be retrieved). This perhaps generalizes to a requirement for a PIP, though that is typically thought to retrieve only environmental data.

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.

Comment: Page: 3
The mechanism for identifying resources must be flexible enough to accommodate resources that are themselves XACML policies.

2.3.4 "Order"

Other discussion that arises in the ebXML use cases is the concept of "order". That is, the policy language needs to be able to express a specific sequence of conditions or policy evaluation.

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. System must evaluate constraints and grant or deny access.

Comment: Page: 3
If it is useful for the requester to be able to know these constraints, then the policies (XACML, P3P, etc.) associated with a resource must be locatable and readable by (at least a portion of) the user population.

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.

Comment: Page: 4
Policy (policies) must be able to state not just who can have access, but also for what purposes (e.g., "may be used for cross-marketing", or "may be combined with this type of data for trends identification/analysis"). [Perhaps this is already addressed by P3P?]

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.

Comment: Page: 4
Policy should have a way of specifying security processing. [More generally, is this the "post-conditions" mechanism in XACL, or is something more specific needed?]

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 Decision Point (PDP) evaluates the policies that apply. The PDP may be located within the server or accessed remotely.

Comment: Page: 4
There may be several policies.

Other use cases in this category include discussion of the protocol to provision a PDP with policy (i.e., the PRP to PDP protocol), and the increasing expressiveness of authorization questions and responses.

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:

Comment: Page: 4
Policy must be able to apply to specific elements as well as to whole documents (i.e., "resource" naming must be flexible enough to specify individual elements).

```
<?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.

Comment: Page: 5
Same as previous comment, but applied to a different action (i.e., action naming must be completely flexible).

Comment: Page: 5
Requirement for labeling (i.e., object/resource "sensitivities").

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.

Comment: Page: 5
Comparison required between holder attributes and resource sensitivity, for a given action.

2.6.4 Paper Reviewing

This application simulates a typical review process for academic papers. This example illustrates how 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.

Comment: Page: 5
Lots of roles (reviewer, program committee, chairperson, rest-of-world). Typically, "world" can't see anything, committee and reviewers can see everything in paper except authors' names / affiliations, chair can see everything, reviewers can't see other reviews, committee and chair can see all reviews, etc. Policy needs to cover elements as well as whole documents, and needs to be able to deal with roles (whose membership may be dynamic).

Comment: Page: 5
Policy created in real time for newly-created resources (by a non-XML expert).

2.6.5 Medical Record

This application illustrates how 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

Comment: Page: 5
Environmental data (such as location of requester) must be taken into account.

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.

Comment: Page: 6
Policy needs to be able to specify what a "valid" document looks like (e.g., "a valid medical record (or consent form) has these two signatures").

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.

Comment: Page: 6
Policies about policies.

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 Access control model for data archives [ACM1]

Enforcing access control at data archives that need to make their data selectively available on the Web. Discussion of data sets and metadata, subject abstractions and profiles, authorizations and restrictions (see document).

Comment: Page: 6
Policy must support access restrictions based on categorizations of users, purposes of use, types of operation, and data objects. These should be definable by the data publisher, and hierarchical structures should be supported. The model should support restrictions, be of declarative form, be simple and expressive, and be easy to use for non-specialists.

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,

Comment: Page: 6
P3P, or similar (i.e., end-user policies or personal preferences).

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

Comment: Page: 6
This may perhaps be accomplished through choices on an organization-provided template.

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.

Comment: Page: 6
Audit logs kept, perhaps for a significant length of time (post-conditions?).

2.9 Workflow [WUC]

Multiple policies (written by different entities) may need to be considered at each stage in the multi-step e-business workflow transaction:

1. Input data needs to be of the "proper" form, with respect to security operations.

2. The data needs to be processed or transformed in some way, with respect to security operations.

3. The resulting data needs to be sent to the next step in the transaction, and relevant security operations need to be performed. In particular, policy regarding "roll-back" (how?, and to what point?) needs to be followed if conditional actions fail.

Comment: Page: 7
Must be able to specify policy regarding roll-back of transactions if pre- or post-conditions fail.

The various policies may be written by the requester, the receiver, the organization, or some other authority. Creation, storage, and acquisition of the relevant policies at the relevant times, policy conflict resolution (if required), and appropriate default behaviours (if a policy is missing) must all be specified.

Comment: Page: 7
Potentially multiple policy authors: requirement for a sophisticated policy evaluation engine.

2.10 Microsoft.NET Stack Walk [MSWUC]

This use case pertains to the execution of software in the Microsoft.NET environment.

At run time, permissions are evaluated based on the execution of code. An assembly, "A3," provides its evidence, along with evidence from the host, to the policy evaluator. The evaluator also takes the permission requests from the assembly into consideration in creating a grant of permissions, "G3." Assembly A3 is called by assembly A2, which has been called by assembly A1. When assembly A3 performs an operation that triggers a security check, the permission grants of A2 and A1 are also examined to ensure that they have the permissions requested by A3. In this process, which is called "stack walking", the permission grants of every assembly on the stack are inspected to see whether the grant set contains the permission demanded by the security check. If each assembly on the stack has been granted the permission demanded by the security check, the call succeeds. If any assembly has not been granted the demanded permission, the stack walk will fail, and a security exception will be thrown.

Comment: Page: 7
Actual requester is only one link in a larger chain; privileges need to be checked for all links. Policy must be able to identify all the links that need to be checked.

2.11 Policy Analysis [PAUC]

Access control policies from stove-piped systems as well as multiple access management systems that may exist inside an enterprise must be brought together an analyzed for policy consistency and adherence to corporate and industry rules and regulations.

2.12 WebDAV [WDAVUC]

(To be submitted by Bill Parducci.)

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

[DRMUC2] Reuters' Requirements for Rights Data Dictionary and Rights Expression Language, David Parrott, June 1, 2001. (See also http://lists.oasis-open.org/archives/xacml/200106/msg00065.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

[WUC] Workflow Use Case http://lists.oasis-open.org/archives/xacml/200109/msg00016.html

[MSWUC] Microsoft Stack Walk Use Case

Taken from document submitted to OASIS SS-TC f2f4 meeting (see also http://lists.oasis-open.org/archives/xacml/200109/msg00040.html).

[PAUC] Policy Analysis Use Case
http://lists.oasis-open.org/archives/xacml/200109/msg00041.html

[WDAVUC] WebDAV Use Case