OASIS eXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE (XACML)

TECHNICAL COMMITTEE

ISSUES LIST

VERSION 1

NOVEMBER 7, 2001

Ken Yagen, Editor

Purpose

This document catalogs issues for the eXtensible Access Control Markup Language (XACML) developed the Oasis eXtensible Access Control Markup Language Technical Committee.

Introduction

The issues list presented here documents issues brought up in response to draft documents as well as other issues mentioned on the xacml mailing list, in conference calls, and in other venues. The structure of this document was taken from the Security Assertion Markup Language (SAML) Issues List document maintained at the Security Services Technical Committee document repository. Each issue is formatted as follows:

ISSUE:[Document/Section Abbreviation-Issue Number: Short name] Issue long description. Possible resolutions, with optional editor resolution Decision

The issues are informally grouped according to general areas of concern. For this document, the "Issue Number" is given as "#-##", where the first number is the number of the issue group.

To make reading this document easier, the following convention has been adopted for shading sections in various colors.

Gray is used to indicate issues that were previously closed.

Blue is used to indicate issues that have just been closed in the most recent revision

Yellow is used to indicated issues which have recently been created or modified or are actively being debated.

Other open issues are not marked, i.e. left white.

Beginning with version 5 of this document, issues with lengthy write-ups, that have been closed "for some time" will be removed from this document, in order to reduce its overall size. The headings, a short description and resolution will be retained. All vote summaries from closed issues have also been removed.

Use Case Issues

Group 1: Group Name

Design Issues

Group 1: Group Name

Policy Model Issues

Group 1: Rules

ISSUE:[PM-1-01: Negative Authorizations]

Authorizations can be either positive (permit) or negative (deny). Should we allow both?

Potential Resolutions:

There seems to be agreement on the fact that the core schema should support positive authorizations only. Negative ones are supported as an extension [Michiharu].

Champion: Michiharu

Status: Open

ISSUE:[PM-1-02: Post-Conditions]

The current schema [Tim, Jan.3] mentions post-conditions, distinguishing between external and internal, depending on whether their execution requires dialoging with external entities. The current schema suggests (via a comment) that post-conditions can be expressed as invocations of SOAP services. Post-conditions are still to be discussed in details:

what is their semantics; how are they executed? A complication of post-conditions associated with a rule involves the distributed scenario (see POLICY COMPOSITION issue). In fact, if I say that a post-condition should be applied whenever a rule fires then I have to evaluate *all* rules.

Potential Resolutions:

???

Champion: ???

Status: Open

Group 2: Applicable Policy

ISSUE:[PM-2-01: Referencing Multiple Policies]

According to the current schema an Applicable Policy seems to refer to a single Policy. The discussions in the last concall seem to assume that an Applicable Policy can refer to several Policies (distributed scenario and multiple issuers [Anne]). Is there agreement on this point? If so, the schema should be modified accordingly.

Potential Resolutions:

???

Champion: Anne

Status: Open

ISSUE:[PM-2-02: Target Specification]

According to the current schema each applicable policy can have multiple targets, each of which is an action and a URI identifying a set of resources (possibly with a transfer function to support wildcards). One may want to specify the target with reference to resource attributes (e.g., this policy applies to all files older that two years). How can I specify this?

Potential Resolutions:

???

Champion: Simon G.

Status: Open

ISSUE:[PM-2-03: Meaningful Actions]

There are pairings <resource,actions> which are not meaningful (e.g., execute a PDF file) [Simon G.]. Should we control resource/action bindings in the language or refer to an external authority?

Potential Resolutions:

???

Champion: Simon G.

Status: Open

ISSUE:[PM-2-04: Indexing Policy]

Also related to target are indexing issues and how to retrieve, given a request, the applicable policy for it [Tim].

Potential Resolutions:

???

Champion: Tim

Status: Open

ISSUE:[PM-2-05: Ensuring Completeness]

The applicable policy is defined as the ``complete'' set of policies that apply to a resource. How do I ensure completeness (meaning no two targets should intersect?)

Potential Resolutions:

???

Champion: ???

Status: Open

Group 3: Policy Composition

Assuming an Applicable Policy can refer to several Policy elements, we need to answer the following questions:

ISSUE:[PM-3-01: Combining Policy Elements]

How are the Policy Element combined? For instance, we could support boolean expressions of policies. E.g., if there are three policies by independent issuers, I can say ``P1 AND (P2 OR P3)? This could fit well in the multiple issuers scenario Anne was envisioning. Should this be part of the core of the extension (external URI [Michiharu])?

Potential Resolutions:

???

Champion: Michiharu

Status: Open

ISSUE:[PM-3-02: Specifying Policy Outcome]

How should the policy outcome be specified. Possibilities are 2-valued (access decision is ``grant"/"deny") or 3-valued (policy outcome is ``grant"/"deny"/nothing). Note the ``nothing" means that no rule applies, to be solved according to default. (related work on composition…?)

Potential Resolutions:

???

Champion: ???

Status: Open

Group 4: Syntax

ISSUE:[PM-4-01: Syntactic Sugar]

The current schema assumes authorizations are specified as a pre-condition which is an expression made of predicates on SAML attributes (conditions on principal, resource and environment can be interspersed), let's call it Option ``pre-cond" [Carlisle, Tim, Anne, ...]. In the last concalls it was agreed to leave as an open issue whether to group conditions about principal, resource, and environment in three different elements, let's call it Option ``triplet" [Michiharu, Ernesto, Simon, ...]. The argument for Option ``pre-cond" is that there are predicates that involve both principal and resource attributes (e.g., an authorization that states that users can read the files they own). The counter-objection to this is that you can naturally include all predicates on resources in the resource condition element (which can also refer to principal attributes). The argument for the triplet is that it makes authorization specifications conceptually clearer and closer to current approaches.

Potential Resolutions:

???

Champion: ???

Status: Open

Group 5: SAML Related

In the current schema attributes on resources and principals, which can be used in the Target (for resources) and in predicates, are retrieved using URIs pointing to SAML dataflow.

ISSUE:[PM-5-01: Non-SAML Input]

Can this mechanism be extended to point to non-SAML authorities as required in the Java

environment [Sehkar]?

Potential Resolutions:

???

Champion: Sehkar

Status: Open

ISSUE:[PM-5-02: Wildcards on Resource Hierarchies]

How do we express wildcards on the resource hierarchies [Simon G.]?

Potential Resolutions:

The current schema includes ResourcetoClassificationTransform to this purpose. Is this sufficient?

Champion: Simon G.

Status: Open

ISSUE:[PM-5-03: Roles and Group Hierarchies]

Are roles and groups hierarchies available via SAML [Simon G.]? Hierarchies could be needed, in case of support of negative rules, for resolving conflicts based on more-specific-takes-precedence. Note: policy resolution conflicts fit well when the principal is a group, they may be difficult to apply in case of principal's expressions.

Potential Resolutions:

???

Champion: Simon G.

Status: Open

ISSUE:[PM-5-04: SAML Assertions URI]

From the schema it seems that expressions are predicates whose arguments are always URI or value. Are SAML assertions always URI?

Potential Resolutions:

???

Champion: ???

Status: Open

ISSUE:[PM-5-05: XPath]

Use of Xpath for identifying SAML constructs and the use of Xpath operators

Potential Resolutions:

???

Champion: ???

Status: Open

ISSUE:[PM-5-06: Multiple actions in single request]

In the SAML issues document, http://www.oasis-open.org/committees/security/docs/draft-sstc-core-discussion-01.doc

... Issue 5.1.15.2 seeks guidance on whether multiple "actions" can be specified in a single decision request.

Potential Resolutions:

[Tim] I feel that XACML should answer this question and send its conclusion in a liaison to SAML. My feeling is that the answer is "No". If "applicable policy" is to be identified with the resource/action pair, then multiple "applicable policies" are involved when multiple actions are involved. Much "cleaner" for there to be a single "applicable policy" for each decision request. And, therefore, a single action per decision request. It is no great hardship to submit multiple decision requests, in the event that you need a decision for each of several actions.

[Hal] Personally I am in favor of limiting this, but I will state the counter argument for the record. If the possible Actions correspond to what can be in the request, then this works fine. The only reason for multiple actions would be some sort of policy provisioning requirement. However, if the Actions are more like privileges or permission bits, and do not match allowable requests one for one, then some requests may require the AND or OR of several actions. I believe this is the motive behind suggesting multiple actions.

I don't see any rush on this as we are not close to proposing changes to the decision protocol yet.

Champion: Tim

Status: Open

ISSUE:[PM-5-07: Delegation]

[Polar] Has anybody thought about how delegation can be reasoned about in XACML? It

appears that SAML only asserts a flat list of attributes with a single principal, or am I off base here? Can I support policies on such operations as:

Paul for Peter says debit Peter's account?

Which mean that Paul (or some other party trusted to do so) has issued Paul the authorization to act on behalf of Peter, in this case to access Peter's account. Or such things, like WebServer quoting JohnDoe says lookup in customer database. Where the WebServer may be trusted to authenticate JohnDoe, but no such proof is necessary other than the WebServer merely claiming to be acting on JohnDoe's behalf?

Potential Resolutions:

[Hal] With regards to SAMl, the Access Decision Request was deliberately kept simple with the idea that XACML would give us the tools to do the job properly. I have preoposed (see my usecases) that XACML not only be able to express policies, but the method of expressing policy inputs be rolled back into the SAML Access Decision Request (and Assertion).

In my opinion, XACML policies should be able to contain predicates about zero or more of the following subjects:

Requestor Subject

Receipient Subject (can be different from requestor)

Intermediary Subject (can be more than one for a given request)

I propose a single construct for Subjects and their attributes and some kind of modifier indicating the type (refrain from using "role" here) of subject.

Champion: Polar/Hal

Status: Open

Group 6: Predicate Cononicalization

ISSUE:[PM-6-01: SAML Assertions URI]

Values used in predicates can refer to various standard formats (e.g, X.509 [Anne]) that could make the predicates evaluation difficult. For instance, if a principal's name is expressed in X.500 syntax you cannot compare it against a simple string. How do we make the representations canonical?

Potential Resolutions:

???

Champion: Anne

Status: Open

Miscellaneous Issues

Group 1: Glossary

ISSUE:[MI-1-01: Consistency]

Pierangela mentioned something discussed in PM group that may not coincide with glossary concerning pre and post conditions.

Potential Resolutions:

???

Champion: Pierangela

Status: Open

Group 2: Conformance

ISSUE:[MI-2-01: Successfully Using]

XACML definition of OASIS requirement to successfully use the specification

Potential Resolutions:

"Successfully Using the XACML Specification"

XACML is an XML schema for representing authorization and entitlement policies. However, it is important to note that a compliant Policy Decision Point (PDP) may choose an entirely different representation for its internal evaluation and decision-making processes. That is, it is entirely permissible for XACML to be regarded simply as a policy interchange format, with any given implementation translating the XACML policy to its own local/native/proprietary/alternate policy language sometime prior to evaluation.

A set of test cases (each test case consisting of a specific XACML policy instance, along with all relevant inputs to the policy decision and the corresponding PDP output decision) will be devised and included on the XACML Web site.

In order to be "successfully using the XACML specification", an implementation MUST, for each test case, have a "policy evaluation component" that can consume the policy instance and the inputs and produce the specified output.

Furthermore, the implementation MUST have a "policy creation component" that allows it to generate schema-valid XACML policy instances that can be consumed/processed by other PDPs.

Note that, aside from the XACML policy instance itself, all PDP inputs and outputs MUST be SAML-compliant (i.e., conform with the assertions and protocol messages defined in the SS-TC SAML specification), although other syntaxes/formats for the PDP input and output MAY be supported in addition to this.

Champion: Carlisle

Status: Closed

Group 3: Patents, IP

ISSUE:[MI-3-01: XrML]

[Ernesto] As I recollect, OASIS requested us to evaluate whether any XACML specification might fall in the scope of patents held by others. I quote from a Dec 13th addition to announcements regarding Xerox's XrML:

(http://xml.coverpages.org/xrml.html) :

"ContentGuard's strategy appears to be to make money by licensing the technology -- whatever some outside body defines it to be. It can do this because its patents cover the idea of a rights language in general, no matter what the specifics of the language are".

I know XrML has already been mentioned in our discussions from the technical point of view, but the wording of this announcements makes me suspect that we should explore the matter further from the patents' point of view.

Potential Resolutions:

???

Champion: Ernesto

Status: Open

Group 4: Other Standards

ISSUE:[MI-4-01: RuleML]

Should XACML look at RuleML?

[Edwin] XACML folks, Since XACML is about defining "rules" for Authorization -- would it make sense to leverage work done by the RuleML folks?

RuleML folks, You may want to checkout XACML as an application of RuleML. Here is a standard that will be real within the next year!]

Potential Resolutions:

???

Champion: Edwin

Status: Open

ISSUE:[MI-4-02: RAD]

Should XACML look at RAD?

[Polar] In response to some query about the expressiveness of evaluation of policies from different places, I would like to point the group to the CORBA Resource Access Decision specification (RAD).

http://www.omg.org/cgi-bin/doc?formal/01-04-11.pdf

and we may want to include it the document repository. It has in it an Access Decision model in which not only policies are located, but also, a policy evaluation combinator is located for a

particular resource. Note, there is no language component to this specification.

However, it does present a model by which policy can be distributed and evaluated. A combinator, which has an interface operation of "evaluate_policies" takes the list of located policies for the resource, the attribute list of the subject, and the operation (i.e. Action) on the resource) and evaluates the decision.

That way, depending the semantics of the combinator you choose for the resource, your combinator may choose to ignore, or evaluate only some policies based on the evaluations of other policies.

Potential Resolutions:

???

Champion: Polar

Status: Open

ISSUE:[MI-4-03: DSML]

Transformations from XACML to DSML

[Gil] Since the last time we talked I had the chance to play with DSML a little. It seems to me

that it is theoretically possible to transform an XACML policy document into a DSML document and import that document into LDAP. The DSML document could contain elements that described the (LDAP) schema necessary to store the authorization policy entries in case the target LDAP

didn't already have this schema. It is also possible to export some LDAP entries into a DSML document and transform that DSML document in XACML.

What I don't know (having nothing more than a cursory understanding of XSL/XSLT) is how difficult such transformations would be and if there are any "gotchas" that would keep this from really working.

Potential Resolutions:

[Gil] What I think the XACML spec should do is:

1.) Describe the LDAP schema necessary to store authorization policies. This should be done in "LDAP fashion" with dn's, classnames, etc.

2.) (if possible) Provide the XSLT necessary to transform XACML to DSML and vice versa.

That way people who don't want to be bothered with DSML can work out their own way to store and retrieve XACML data to and from the defined schema.

Champion: Gil

Status: Open

Document History

- 7 Jan 2002 First Version Published