Conformance Program Specification for the OASIS eXtensible Access Control Markup Language (XACML)

Document identifier: draft-xacml-conform-spec-01

Location: http://www.oasis-open.org/committees/xacml/docs

Publication date: 17 April 2002

Maturity Level: Committee Draft

Send comments to: xacml-comment@lists.oasis-open.org *unless* you are subscribed to the XACML list for committee members -- send comments there if so. Note: Before sending messages to the xacml-comment list, you must first subscribe. To subscribe, send an email message to xacml-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

Editors:

Ken Yagen, CrossLogix

Contributors:

Tim Moses, Entrust
Anne Anderson, Sun Microsystems
Bill Parducci, Bill Parducci
Carlisle Adams, Entrust
Ernesto Damiani, University of Milan
Hal Lockhart, Entegrity
Michiharu Kudo, IBM, Japan
Pierangela Samarati, University of Milan
Polar Humenn, Syracuse University
Sekhar Vajjhala, Sun Microsystems
Simon Godik, Simon Godik

Rev	What
001	Initial version

1 Introduction

This document describes the program and technical requirements for the XACML conformance system. Since XACML is an extension schema for SAML, this document borrows heavily from the Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML) [SAML Conf].

1.1 Scope of the Conformance Program

XACML deals with several components from policy creation to policy evaluation. Not all software might choose to implement all the XACML specifications. In order to achieve compatibility and interoperability, applications and software need to be certified for conformance in a uniform manner. The XACML conformance effort aims at fulfilling this need.

The deliverables of the XACML conformance effort include:

- Conformance Clause, defining at a high-level what conformance means for the XACML standard
- Conformance Program specification, defining how an implementation or application establishes conformance
- Conformance Test Suite. This is a set of test programs, result files and report generation tools that can be used by vendors of XACML-compliant software, buyers interested in confirming XACML compliance of software, and testing labs running conformance tests on behalf of vendors or buyers.

Section 2 of this document provides the XACML Conformance Clause. Section 3 deals with defining and specifying the process by which conformance to the XACML specification can be demonstrated and certified. Section 4 elaborates the technical requirements which constitute conformance; this includes both the levels of conformance that may be demonstrated and the requirements for each of those levels of conformance. Section 5 describes the test suite for XACML, including the processes for using the test suite to establish conformance, and the policies and procedures relating to those processes. Section 6 defines the services which are available to assist in establishing conformance.

1.2 Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 **[NIST/ITL]** “What is this thing called conformance” [Rosenthal, Brady; NIST/ITL Bulletin, January 2001] http://www.itl.nist.gov/div897/ctg/conformance/bulletin-conformance.htm.

[RFC2119].

2 Conformance Clause

The objectives of the XACML Conformance Clause are to:

1. Ensure a common understanding of conformance and what is required to claim conformance
2. Promote interoperability in the exchange of policy statements
3. Promote uniformity in the development of conformance tests

The XACML Conformance Clause specifies explicitly all the requirements that have to be satisfied to claim conformance to the XACML standard.

2.1 Specification of the XACML Standard

The following specifications, in addition to this XACML conformance program specification, comprise the proposed Version 1.0 specification for the XACML standard:

- OASIS eXtensible Access Control Markup Language (XACML)
- Security Considerations for the OASIS eXtensible Access Control Markup Language (XACML)
- Glossary for the OASIS eXtensible Access Control Markup Language (XACML)

Although additional documents might use or reference the XACML standard (such as white papers, descriptions of custom profiles, and position papers referencing particular issues), they do not constitute part of the standard.

2.2 Declaration of XACML Conformance

Conformance to the XACML standard may be declared for the entire standard or for a subset of the standard, based on the requirements that a given implementation or application claims to meet. That is, requirements can be applied at varying levels, so that a given implementation or application of the XACML standard can achieve clearly defined conformance with all or part of the entire set of specifications.

Conformance claims MAY be made by either one of two components in the XACML model:

1. An implementation of a policy administration points that produces policy statements that conform with the XACML schema; and

2. An implementation of a policy decision point that produces decisions in response to decision requests on the basis of XACML policy statements that conform with the XACML schema.

In the current version of the specification, implementations of a policy retrieval point that produce policy statements that conform with the XACML schema by combining XACML applicable policies are treated in the same way as policy administration points, from the point of view of conformance.

Policy administration points MAY claim conformance with the XACML specification provided merely that they produce schema-compliant policy statements.

Policy decision points MAY claim conformance with the XACML specification provided that they correctly execute the XACML conformance test suite provided:

http://www.oasis-open.org/ …

An application or implementation should express its level of conformance in terminology such as the following:

[Application or implementation] as both PAP and PDP supports all XACML policy syntax and combining algorithms. It also supports the SAML Profile. No optional elements for the extension points are implemented.

2.3 Mandatory/Optional Elements in XACML Conformance

2.4 Impact of Extensions on XACML Conformance

XACML supports extensions. An application or implementation may claim conformance to XACML only if its extensions (if any) meet the following requirements:

- Extensions shall not re-define semantics for existing functions.
- Extensions shall not alter the specified behavior of interfaces defined in this standard.
- Extensions may add additional behaviors.
- Extensions shall not cause standard-conforming functions (i.e., functions that do not use the extensions) to execute incorrectly.

XACML can be extended so long as the above conditions are met. It is requested that, if a system is extending XACML:

- The mechanism for determining application conformance and the extensions shall be clearly described in the documentation, and the extensions shall be marked as such;
- Extensions shall follow the spirit, principles and guidelines of the XACML specification, that is, the specifications must be extended in a standard manner as defined in the extension fields.
- In the case where an implementation has added additional behaviors, the implementation shall provide a mechanism whereby a conforming application shall be recognized as such, and be executed in an environment that supports the functional behavior defined in this standard

Extensions are outside the scope of conformance. There are no mechanisms specified to validate and verify the extensions. This section contains the recommended guidelines for extensions.

2.5 Conformance with SAML

TBD

3 Conformance Process

As discussed in the article “What is this thing called conformance” **[NIST/ITL]**, conformance can comprise any of several levels of formal process:

- **Conformance testing** (also called conformity assessment) is the execution of automated or non-automated scripts, processes or other mechanisms to determine whether an application or implementation of a specification deviates from that specification. For XACML, conformance testing means the running of (some or all) tests within the XACML Conformance Test Suite. Conformance testing performed by implementers early on in the development process can find and correct their errors before the software reaches the marketplace, without necessarily being part of either a validation or certification process.
- **Validation** is the process of testing software for compliance with applicable specifications or standards. The validation process consists of the steps necessary to perform the conformance testing by using an official test suite in a prescribed manner.
- **Certification** is the acknowledgment that a validation has been completed and the criteria established by the certifying organization for issuing a certificate have been met. Successful completion of certification results in the issuance of a certificate (or brand) indicating that the implementation conforms to the appropriate specification. It is important to note that certification cannot exist without validation, but validation can exist without certification.

The conformance process for XACML is based on validation rather than certification. That is, no certifying organization has been established with the responsible for issuing a statement of conformance with regard to an application or implementation. Therefore, an implementer who has validated XACML conformance by means of conformance testing may not legitimately use the term “certified for XACML conformance”. Until and if a certification process is in place, vendor declaration of validation will be the only means of asserting that conformance testing has been performed.

The conformance process does not stipulate whether validation is performed by the implementer, by a third-party, or by the customer of an application or implementation. Rather, the conformance process describes the way in which conformance testing should be done in order to demonstrate that an application or implementation correctly performs the functionality specified in the standard. Validation achieved through the XACML conformance process provides software developers and users assurance and confidence that the product behaves as expected, performs functions in a known manner, and possesses the prescribed interface or format.

The XACML Technical Committee is responsible for generating the materials that allow vendors, customers, and third parties to evaluate software for XACML conformance. These materials include:

- Documentation describing test cases, linked to use cases and requirements
- Test suite, based on those test cases, that can be run against an implementation to demonstrate any of the several levels of conformance defined in the conformance clause of the XACML specification
- Documentation describing how to run the test suite, interpret the results, and resolve disputes regarding the results of the tests

The XACML Technical Committee is not, however, responsible for testing of particular implementations.

3.1 Implementation and Application Conformance

XACML Conformance is applicable to:

- Implementations of XACML components. These could be in the form of toolkits, products incorporating XACML components, or reference implementations that demonstrate the use of XACML components.

- Applications that produce or consume XACML policy statements or that evaluate XACML policy statements.

A conforming **implementation** shall meet all the following criteria:

4. The implementation shall support all the required interfaces defined within this standard for a given component. The implementation shall support the functional behavior described in the standard.
5. An implementation may provide additional or enhanced features or functionality not required by the XACML Specification. These non-standard extensions shall not alter the specified behaviour of interfaces or functionality defined in the specification.
6. The implementation may provide additional or enhanced facilities not required by this standard. These non-standard extensions shall not alter the specified behavior of interfaces defined in this standard. They may add additional behaviors. In these circumstances, the implementation shall provide a mechanism whereby a XACML conforming application shall be recognized as such, and be executed in an environment that supports the functional behavior defined in this standard.

A conforming **application** shall meet all the following criteria:

1. The application shall be able to execute on any conforming implementation.
2. If an application requires a particular feature set that is not available on a specific implementation, then the application must act within the bounds of the XACML specification even though that means that the application may not perform any useful function. Specifically, the application shall do no harm, and shall correctly return resources and vacate memory upon discovery that a required element is not present.

3.2 Process for Declaring Conformance

The following process should be followed in declaring that an application or implementation conforms to the XACML standard:

1. Determine which bindings and protocols will be asserted as conforming.
2. Obtain the test suite for the XACML standard from [tbs]
3. Validate the application or implementation by execute those conformance tests from the test suite which are relevant to the conformance being asserted.
4. Send the statement claiming conformance to the XACML Technical Committee at [tbs] so that it can be posted on the XACML web site. A statement of any profiles which are being used that are not part of the XACML standard should also be sent to the XACML Technical Committee at the same time for posting on the XACML web site.

4 Technical Requirements for XACML Conformance

This section defines the technical criteria which apply to declaring conformance to the XACML standard. The requirements are specified as test cases.

Each test case includes:

- A description of the test purpose (that is, what is being tested – the conditions, requirements, or capabilities which are to be addressed by a particular test)
- The pass/fail criteria
- A reference to the requirement in the requirements document relevant to the test case
- A reference to the section in the standard from which the test case is derived (that is, traceability back to the specification)

For each assertion, both required tests for producing and consuming the policy statements, as well as tests related to profiles are specified.

…

5 Test Suite

A test suite, which is the combination of test cases and test documentation, is used to check whether an implementation or application satisfies the requirements in the standard. The test cases, implemented by a test tool or a set of files (i.e., data, programs, scripts, or instructions for manual action) checks each requirement in the specification to determine whether the results produced by the implementation or application match the expected results, as defined by the specification.

The test documentation describes how the testing is to be done and the directions for the tester to follow. Additionally, the documentation should be detailed enough so that testing of a given implementation can be repeated with no change in test results.

Conformance testing is black box testing to test the functionality of an implementation. This means that the internal structure or the source code of a candidate implementation is not available to the tester. However, content and format of received or returned messages can be inspected as part of the determination of conformance.

The test suite for XACML should be platform independent, non-biased, objective tests. Generally a conformance test suite is a collection of combinations of legal and illegal inputs to the implementation being tested, together with a corresponding collection of expected results. Only the requirements specified in the standard are testable. A test suite should not check any implementation properties that are not described by the standard or set of standards. A test suite cannot require features that are optional in a standard, but if such features are present, a test suite could include tests for those features. A test suite does not assess the performance of an implementation unless performance requirements are specified in the specification, although implementation dependencies or machine dependencies may be demonstrated through the execution of the test cases.

The results of conformance testing apply only to the implementation and environment for which the tests are run. Test suites may be provided as a web-based system executed on a remote server, downloadable files for local execution, or a combination of remote and local access and execution. The method for providing and delivering the test suite depends on what is being tested as well as the objective for test suite use – that is, providing self-test capability or formal certification testing.

The test suite comprises three directories:

- Decision requests
- Policies
- Authentication and attribute assertions
- Decision assertions

The decision requests directory contains a set of text/xml/samlp files that are valid SAML authorization decision request messages.

The polices directory contains precisely one XACML policy file whose target includes includes each of the decision requests.

The assertions directory contains an unordered set of text/xml/saml files containing the attributes required to evaluates the policies in the policies directory.

The decisions directory contains an unordered set of tect/xml/samlp files that are valid SAML authorization decision responses.

A conformant XACML ***PDP*** implementation shall create a decision assertion in response to each and every decision request. The decision responses are linked to the corresponding decision requests by the request ID attribute.

XACML implementations that target an application domain other than SAML may use a tool or process that is not an integral part of the implementation to convert between the SAML test vectors and its private data representation.

Disclaimer: Implementors SHALL NOT consider the test cases provided in the XACML conformance test suite as providing 100% test coverage. OASIS does not represent that a conformant implementation will operate correctly in all respects nor that it is fit for its purpose.

As a test suite for XACML becomes available, the following information will be provided:

- Reference Architecture
- Infrastructure
- Using the test suite
- Test result tabulation and reporting

The XACML test suite will be maintained on a best-effort basis.

6 Conformance Services

The OASIS XACML Technical Committee does not itself provide conformance services. As the XACML test suite becomes available and experience with XACML identified appropriate conformance testing approaches, the Conformance Specification will describe the services which the organization should provide including software services, releases, self-test kit, actual computer systems, facilities, web based interfaces, and availability.

7 References

[NIST/ITL] “What is this thing called conformance” [Rosenthal, Brady; NIST/ITL Bulletin, January 2001] http://www.itl.nist.gov/div897/ctg/conformance/bulletin-conformance.htm.

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[XACML Core] T. Moses et al., *OASIS eXtensible Access Control Markup Language (XACML)*, http://www.oasis-open.org/committees/xacml/docs/, OASIS, March 2002.

[SAMLConf] R Griffin et al., *Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/docs/draft-sstc-conform-spec-12.pdf, OASIS, March 2002.

Appendix A. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Appendix B. Issues