XACML v3.0 XML Digital Signature Profile Version 1.0

Committee Draft 01

16 April 2009

Specification URIs:
This Version:
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-dsig-v1-spec-cd-1-en.html
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-dsig-v1-spec-cd-1-en.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-dsig-v1-spec-cd-1-en.pdf

Previous Version:
N/A

Latest Version:
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-dsig-v1-spec-en.html
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-dsig-v1-spec-en.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-dsig-v1-spec-en.pdf

Technical Committee:
OASIS eXtensible Access Control Markup Language (XACML) TC

Chair(s):
Hal Lockhart, BEA <hlockhar@bea.com>
Bill Parducci, <bill@parducci.net>

Editor(s):
Erik Rissanen, Axiomatics AB <erik@axiomatics.com>

Related work:

This specification replaces or supercedes:

- XML Digital Signature Profile of XACML 2.0

This specification is related to:

- eXtensible Access Control Markup Language (XACML) Version 3.0, wd 11

Declared XML Namespace(s):

None

Abstract:

This specification profiles use of the W3C XML-Signature Syntax and Processing Standard in providing authentication and integrity protection for XACML schema instances.

Status:

This document was last revised or approved by the OASIS eXtensible Access Control Markup Language (XACML) TC on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at http://www.oasis-open.org/committees/xacml/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/xacml/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/xacml/.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

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 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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 any document or deliverable produced by an OASIS Technical Committee can be found on 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 OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS" and “XACML” are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

This document provides a profile for use of the W3C XML-Signature Syntax and Processing Standard in providing authentication and integrity protection for OASIS eXtensible Access Control Markup Language **[XACML]** schema instances. Sections 9.2.1 Authentication and 9.2.4 Policy integrity in **[XACML]** describe requirements and considerations for such authentication and integrity protection.

A digital signature is useful for authentication and integrity protection only if the signed information includes a specification of the identity of the signer and a specification of the period during which the signed ***data object*** is to be considered valid. XACML itself does not define the format for such information, as XACML is intended to use other standards for functions other than the actual specification and evaluation of access control policies, requests, and responses.

One appropriate format that has been defined elsewhere is **[SAML]**. A profile for the use of SAML with XACML schema instances is available in **[XACML-SAML]**. This profile therefore RECOMMENDS use of XACML schema instances in SAML Assertions, Requests, and Responses, which MAY then be digitally signed as specified in the SAML specification.

This profile also notes various canonicalization issues that must be resolved in order for signed documents to be verified by a relying party.

This profile specification assumes that the reader is familiar with the concept of a digital signature, with the W3C XML-Signature Syntax and Processing Standard, and with XACML.

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

1.2 Glossary

Data object

Used in this profile to refer to a digital object that is being signed. A ***data object*** could be an XACML PolicySet, Policy, Request context, Response context, or any associated schemas. A ***data object*** is referenced inside an **[XMLDSIG]** `<Reference>` element using a URI as defined by **[RFC2396]**.

1.3 Normative References

[ExclC14N] J. Boyer et al., *Exclusive Canonicalization Version 1.0*, 18 January 2002, World Wide Web Consortium, http://www.w3.org/TR/xml-exc-c14n/.

[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.

[RFC2253] M. Wahl, et al., *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*, IETF RFC 2253, September 1997, http://www.ietf.org/rfc/rfc2253.txt.

[RFC2396] T. Berners-Lee, et al., *Uniform Resource Identifiers (URI): Generic Syntax,* August 1998, ftp://ftp.isi.edu/in-notes/rfc2396.txt.

[SAML] S. Cantor, et al., eds., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML} V2.0*, http://www.oasis-open.org/committees/documents.php?wg_abbrev=security.

[ScC14N] S. Aissi, M. Hondo, eds., *Schema Centric XML Canonicalization, Version 1.0*, 20 May 2003, http://uddi.org/pubs/SchemaCentricCanonicalization.htm.

[XACML] E. Rissanen, ed., *eXtensible Access Control Markup Language (XACML) Version 3.0*, Working Draft 11, 5 April 2009, FIXME URL.

[XACML-SAML] H. Lockhart, et al, eds., *SAML 2.0 profile of XACML, Version 2*, Working Draft 8, 5 April 2009, FIXME URL.

[XMLDSIG] D. Eastlake, et al., *W3C XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002, http://www.w3.org/TR/xmldsig-core.

[XPath2Filt] J. Boyer, M. Hughes, J. Reagle, editors, *XML-Signature XPath Filter 2.0*, 8 November 2002 http://www.w3.org/TR/xmldsig-filter2/.

[X.690] ITU-T Recommendation X.690 Information Technology – Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: General procedures, 1992.

1.4 Non-Normative References

None

2 XML Digital Signature profile of XACML

2.1 Use of SAML

This Profile RECOMMENDS use of XACML schema instances embedded in SAML Assertions, Requests, and Responses as described in **[XACML-SAML]**. Such SAML objects SHALL be digitally signed as described in Section 5: SAML and XML Signature Syntax and Processing of **[SAML]**.

2.2 Canonicalization

In order for a digital signature to be verified by a relying party, the byte stream that was signed MUST be identical to the byte stream that is verified. To ensure this, the XML document being signed MUST be canonicalized. Section 5: SAML and XML Signature Syntax and Processing of **[SAML]** specifies use of Exclusive Canonicalization **[ExclC14N]**.

2.2.1 Namespace elements in XACML data objects

Any XACML ***data object*** that is to be signed MUST specify all namespace elements used in the ***data object***. If this is not done, then the ***data object*** will attract namespace definitions from ancestors of the ***data object*** that may differ from one envelope to another.

When **[ExclC14N]** is used as the canonicalization or transform method, then the namespace of XACML schemas used by elements in an XACML ***data object*** MUST be bound to prefixes and included in the InclusiveNamespacesPrefixList parameter to **[ExclC14N]**.

2.2.2 Additional canonicalization considerations

Additional transformations on the XACML ***data object*** must usually be performed in order to ensure that the ***data object*** signed will match the ***data object*** that is verified. Some of these transformations are listed here, but this Profile does not attempt to specify algorithms for performing these.

If an XACML ***data object*** includes data elements that may be represented in more than one form (such as (TRUE, FALSE), (1,0), (true,false)), then a Transform method MUST be defined and specified for normalizing those data elements.

This Profile RECOMMENDS applying the following canonicalizations to values of the corresponding datatypes, whether occurring in XML attribute values or in XACML Attributes.

1. Where a canonical representation for an XACML-defined datatype is defined in http://www.w3.org/2001/XMLSchema, then the value of the datatype MUST be put into the canonical form specified in http://www.w3.org/2001/XMLSchema. This includes boolean {“true”, “false”}, double, dateTime, time, date, and hexBinary (upper-case).
2. http://www.w3.org/2001/XMLSchema#anyURI - use the canonical form defined in **[RFC2396]**
3. http://www.w3.org/2001/XMLSchema#base64Binary - remove all line breaks and white space. Remove all characters following the first sequence of “=” characters. The Base64 Transform (identifier: http://www.w3.org/TR/xmldsig-core/#sec-Base-64) MAY be useful in performing this canonicalization.

urn:oasis:names:tc:xacml:1.0:data-type:x500Name - first normalize according to **[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.

4. **[RFC2253]**. If any RDN contains multiple attributeTypeAndValue pairs, re-order the AttributeValuePairs in that RDN in ascending order when compared as octet strings (described in Section 11.6 “Set-of components” of **[X.690]**).
5. urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name - normalize the domain-part of the name to lower case.

6. XPath expression – apply **[XPath2Filt]** to put the XPath expression into canonical form.

Schema Centric XML Canonicalization Version 1.0 **[ScC14N]** describes many canonicalization issues for XML documents that should be addressed.

2.3 Signing schemas

The parsing of any XACML ***data object*** depends on having an accurate copy of all schemas on which the XACML ***data object*** depends. Note that the inclusion of a schema URI in the XACML schema instance attributes does not guarantee that an accurate copy of the schema will be used: an attacker may substitute a bogus schema that contains the correct identifier. Signatures can help protect against substitution or modification of the schemas on which an XACML ***data object*** depends. Use of signatures for this purpose are described in this section.

In most cases, a ***data object*** signer SHOULD include a `<Reference>` element for each schema on which the XACML ***data object*** depends in the `<SignedInfo>` element that contains the `<Reference>` to or including the XACML ***data object*** itself.

In some cases, the ***data object*** signer knows that all PDPs that will evaluate a given XACML ***data object*** will have accurate copies of certain schemas needed to parse the ***data object***, and does not want to force the PDP to verify the message digest for such schemas. In these cases the ***data object*** signer MAY omit `<Reference>` elements for any schema whose verification is not needed.

3 Conformance

In implementation may conform as a producer and/or a consumer of signed policies.

3.1 As a producer of signed policies

An implementation conforms to this specification as a producer if it is able to produce XACML policies with XML digital signatures as specified in section 2 of this document.

3.2 As a consumer of signed policies

An implementation conforms to this specification as a consumer if it is able to consume XACML policies with XML digital signatures as specified in section 2 of this document.

A. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Anthony Nadalin
Bill Parducci
Daniel Engovatov
Erik Rissanen
Hal Lockhart
Michiharu Kudo
Michael McIntosh
Steve Anderson
Tim Moses

B. Revision History

[optional; should not be included in OASIS Standards]

Revision	Date	Editor	Changes Made
WD 1		Erik Rissanen	Initial conversion to XACML 3.0.
WD 2	24 December 2007	Erik Rissanen	Convert to current OASIS template.
WD 3	4 April	Erik Rissanen	Editorial cleanups