eXtensible Access Control Markup Language (XACML) Version 3.0 Errata 01

Committee Specification Draft 01 / Public Review Draft 01

16 February 2017

Specification URIs

This version:

http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01.doc (Authoritative)

http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01.html

http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/xacml/3.0/errata01/xacml-3.0-core-spec-errata01.doc (Authoritative)

http://docs.oasis-open.org/xacml/3.0/errata01/xacml-3.0-core-spec-errata01.html

http://docs.oasis-open.org/xacml/3.0/errata01/xacml-3.0-core-spec-errata01.pdf

Technical Committee:

OASIS eXtensible Access Control Markup Language (XACML) TC

Chairs:

Bill Parducci (bill@parducci.net), Individual

Hal Lockhart (hal.lockhart@oracle.com), Oracle

Editor:

Richard C. Hill (Richard.C.Hill@boeing.com), The Boeing Company

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

- *eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01 (redlined)*. OASIS Standard change-marked (redlined) with Public Review Draft 01 of Errata 01: http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01-redlined.html.
- *eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01*. OASIS Standard incorporating Public Review Draft 01 of Errata 01: http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01-complete.html.
- XML schema – unmodified from OASIS Standard: http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/schema/xacml-core-v3-schema-wd-17.xsd.

Related work:

This specification provides Errata for:

- *eXtensible Access Control Markup Language (XACML) Version 3.0.* Edited by Erik Rissanen. 22 January 2013. OASIS Standard. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

Declared XML namespace:

- urn:oasis:names:tc:xacml:3.0:core:schema:wd-17

Abstract:

This document lists Errata for the OASIS Standard *eXtensible Access Control Markup Language (XACML) Version 3.0.*

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" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://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 TC's web page (https://www.oasis-open.org/committees/xacml/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

When referencing this specification the following citation format should be used:

[XACML-v3.0-Errata01]

eXtensible Access Control Markup Language (XACML) Version 3.0 Errata 01. Edited by Richard C. Hill. 16 February 2017. OASIS Committee Specification Draft 01 / Public Review Draft 01. http://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01.html. Latest version: http://docs.oasis-open.org/xacml/3.0/errata01/xacml-3.0-core-spec-errata01.html.

Notices

Copyright © OASIS Open 2017. All Rights Reserved.

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 name "OASIS" is a trademark 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 https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

[All text is normative unless otherwise labeled]

1.1 Normative References

[XACML3]   OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version 3.0", January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.doc

1.2 Non-Normative References

[INFOSET]   XML Information Set (Second Edition), W3C Recommendation 4 February 2004, available at https://www.w3.org/TR/xml-infoset/

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

2 Approved Errata

The following are the approved errata to the OASIS XACML v3.0 standard.

2.1 Definition of Target

Change to section 1.1.1 Preferred terms, line 91 - 93, page 11

Remove:

Target

The set of *decision requests*, identified by definitions for *resource*, *subject* and *action* that a *rule*, *policy,* or *policy set* is intended to evaluate

Add:

Target

An element of an XACML *rule*, *policy*, or *policy set* which matches specified values of *resource*, *subject*, *environment*, *action*, or other custom attributes against those provided in the request context as a part of the process of determining whether the *rule*, *policy*, or *policy set* is applicable to the current decision.

2.2 Reference to INFOSET

Change to section 1.4 Normative References, page 12

Add:

[INFOSET]   XML Information Set (Second Edition), W3C Recommendation
4 February 2004, available at https://www.w3.org/TR/xml-infoset/

2.3 Namespace Context for XPath Expressions

Change to section 5.30, line 2494, page 59

Add:

The namespace context for the value of the Path attribute is given by the [in-scope namespaces] **[INFOSET]** of the <AttributeSelector> element.

Change to section A.2 Data-types, lines 4050 - 4052, page 106

Remove:

When the value is encoded in an <AttributeValue> element, the namespace context is given by the <AttributeValue> element and an XML attribute called XPathCategory gives the category of the <Content> element where the expression applies.

Add:

When the value is encoded in an <AttributeValue> element, the namespace context is given by the [in-scope namespaces] (see **[INFOSET]**) of the <AttributeValue> element, and an XML attribute called XPathCategory gives the category of the <Content> element where the expression applies.

2.4 Number of Minor Status Codes

Change to section 5.55, lines 3025 - 3026, page 71

Remove:

The <StatusCode> element contains a major status code value and an optional sequence of minor status codes.

Add:

The <StatusCode> element contains a major status code value and an optional recursive series of minor status codes.

2.5 Keyword Usage

Change to section A.3.5 Logical functions, line 4259, page 111

Remove:

Note: When evaluating and, or, or n-of, it MAY NOT be necessary to attempt a full evaluation of each

Add:

Note: When evaluating and, or, or n-of, it may not be necessary to attempt a full evaluation of each

2.6 Policy Identifier List

Change to section 5.48, lines 2922 - 2925

Remove:

If the ReturnPolicyIdList attribute in the <Request> is true (see section 5.42), a PDP that implements this optional feature MUST return a list of all policies which were found to be fully applicable. That is, all policies where both the <Target> matched and the <Condition> evaluated to true, whether or not the <Effect> was the same or different from the <Decision>.

Add:

If the ReturnPolicyIdList attribute in the <Request> is true (see section 5.42), a PDP that implements this optional feature MUST return a list which includes the identifiers of all policies which were found to be fully applicable, whether or not the <Effect> was the same or different from the <Decision>. The list MAY include the identifiers of other polices which are currently in force, as long as no policies required for the decision are omitted. A PDP MAY satisfy this requirement by including all policies currently in force, or by including all policies which were evaluated in making the decision, or by including all policies which did not evaluate to

"NotApplicable", or by any other algorithm which does not omit any policies which contributed to the decision. However, a decision which returns "NotApplicable" MUST return an empty list.

2.7 Attribute Selector Result

Change to section 5.30, lines 2499 – 2500, page 59

Remove:

This attribute governs whether the element returns "Indeterminate" or an empty bag in the event the XPath expression selects no node.

Add:

This attribute governs whether the element returns "Indeterminate" or an empty bag in the event that the attributes category specified by the Category attribute does not exist in the request context, or the attributes category does exist but it does not have a <Content> child element, or the <Content> element does exist but the XPath expression selects no node.

Change to section 7.3.7, lines 3326 - 3327, page 79

Remove:

1. Construct an XML data structure suitable for xpath processing from the <Content> element in the attributes category given by the Category attribute.

Add:

1. If the attributes category given by the Category attribute is not found or does not have a <Content> child element, then the return value is either "Indeterminate" or an empty bag as determined by the MustBePresent attribute; otherwise, construct an XML data structure suitable for xpath processing from the <Content> element in the attributes category given by the Category attribute.

Change to section 7.3.7, line 3346, page 79

Add:

If the evaluation returns an empty sequence of nodes, then the return value is either "Indeterminate" or an empty bag as determined by the MustBePresent attribute.

2.8 Spurious start-tag

Change to section 5.44, line 2808, page 66

Remove:

</xs:complexType><xs:complexType name="SubjectType">

Add:

</xs:complexType>

2.9 Relocate Attributes Text

Change to section 5.42 Element <Request>, lines 2744 - 2747, page 65

Remove:

> The <Request> element contains <Attributes> elements. There may be multiple <Attributes> elements with the same Category attribute if the PDP implements the multiple decision profile, see [Multi]. Under other conditions, it is a syntax error if there are multiple <Attributes> elements with the same Category (see Section 7.19.2 for error codes).

Change to section 5.42 Element <Request>, following line 2776, page 65

Add:

> The <Request> element contains <Attributes> elements. There may be multiple <Attributes> elements with the same Category attribute if the PDP implements the multiple decision profile, see [Multi]. Under other conditions, it is a syntax error if there are multiple <Attributes> elements with the same Category (see Section 7.19.2 for error codes).

3 Conformance

This document does not add any additional conformance requirements.

Appendix A. Acknowledgments

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

Participants:
>Erik Rissanen, Axiomatics
>Bill Parducci, Individual Member
>Martin Smith, Individual Member
>Rich Levinson, Oracle
>Hal Lockhart, Oracle
>Richard C. Hill, The Boeing Company
>Mohammad Jafari, Veterans Health Administration
>Steven Legg, ViewDS Identity Solutions

Appendix B. Revision History

Revision	Date	Editor	Changes Made
WD1	10/31/2016	Richard Hill	Initial committee draft
WD2	12/18/2016	Richard Hill	Updates to WD1 based on TC comments, which includes updates to references, Definition of Target, Namespace Context for XPath Expressions, and added Relocate Attributes Text section.
WD3	1/3/2017	Richard Hill	Added Reference to INFOSET section, moved [INFOSET] and [RFC2119] references to the non-normative references section, removed the terminology section.
WD4	1/19/2017	Richard Hill	Updated section 2.2 to bold **[INFOSET]**. Added Mohammad Jafari to participants list