XACML v3.0 Privacy Policy Profile Version 1.0

Committee Specification Draft 05 / Public Review Draft 03

16 October 2014

Specification URIs

This version:

http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd03/xacml-3.0-privacy-v1.0-csprd03.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd03/xacml-3.0-privacy-v1.0-csprd03.html
http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd03/xacml-3.0-privacy-v1.0-csprd03.pdf

Previous version:

http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd02/xacml-3.0-privacy-v1.0-csprd02.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd02/xacml-3.0-privacy-v1.0-csprd02.html
http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd02/xacml-3.0-privacy-v1.0-csprd02.pdf

Latest version:

http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/xacml-3.0-privacy-v1.0.doc (Authoritative)
http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/xacml-3.0-privacy-v1.0.html
http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/xacml-3.0-privacy-v1.0.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:

Erik Rissanen (erik@axiomatics.com), Axiomatics

Related work:

This specification replaces or supersedes:

- *Privacy policy profile of XACML v2.0*. Edited by Tim Moses. 1 February 2005. OASIS Standard. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-privacy_profile-spec-os.pdf.

This specification is related to:

- *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.

Abstract:

This specification describes a profile of XACML for expressing privacy policies.

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 Technical Committee web page (https://www.oasis-open.org/committees/xacml/ipr.php).

Citation format:

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

[xacml-3.0-privacy-v1.0]

XACML v3.0 Privacy Policy Profile Version 1.0. Edited by Erik Rissanen. 16 October 2014. OASIS Committee Specification Draft 05 / Public Review Draft 03. http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/csprd03/xacml-3.0-privacy-v1.0-csprd03.html. Latest version: http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/xacml-3.0-privacy-v1.0.html.

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 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

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

Custodian

The entity to which personally-identifiable information is entrusted.

Owner

The subject of personally-identifiable information.

1.3 Normative References

[Hier] *XACML v3.0 Hierarchical Resource Profile Version 1.0*. 10 August 2010. OASIS Committee Specification 01. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-hierarchical-v1-spec-cs-01-en.doc

[OECD] “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, OECD, 1980. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[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 Privacy Guidelines - Organization of Economic Cooperation and Development, 1980 (Non-normative)

The following extract from **[OECD]** describes the obligations on the custodian.

1. **Openness.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data quality principle.** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose specification.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use limitation principle.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
    a. with the consent of the data subject; or
    b. by the authority of law.
5. **Security safeguards principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.
7. **Individual participation principle.** An individual should have the right:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have communicated to him, data relating to him
        i. within a reasonable time;
        ii. at a charge, if any, that is not excessive;
        iii. in a reasonable manner; and
        iv. in a form that is readily intelligible to him;
    c. to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    d. to challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended.
8. **Accountability principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

This profile provides standard attributes and a standard `<Rule>` element for enforcing the 3rd and 4th principles, related to the purpose for which personally identifiable information is collected and used.

3 Standard attributes

This profile defines two attributes.

"urn:oasis:names:tc:xacml:2.0:resource:purpose"

> This attribute, of type "http://www.w3.org/2001/XMLSchema#string", indicates the purpose for which the data resource was collected. The owner of the resource SHOULD be informed and consent to the use of the resource for this purpose. The attribute value MAY be a regular expression. The custodian's privacy policy SHOULD define the semantics of all available values.

"urn:oasis:names:tc:xacml:2.0:action:purpose"

> This attribute, of type "http://www.w3.org/2001/XMLSchema#string", indicates the purpose for which access to the data resource is requested. Action purposes MAY be organized hierarchically, in which case the value MUST represent a node in the hierarchy. See **[Hier]**.

4 Example rules (Non-normative)

4.1 Matching purpose

This rule must be used with the “urn:oasis:names:tc:xacml:2.0:rule-combining-algorithm:deny-overrides” rule-combining algorithm. It stipulates that access shall be denied unless the purpose for which access is requested matches, by regular-expression match, the purpose for which the data resource was collected.

```
<Rule xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance";
  xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17
   xacml-core-v3-schema-wd-17.xsd"
  RuleId="urn:oasis:names:tc:xacml:2.0:matching-purpose"
  Effect="Deny">
<Condition>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of-any">
     <Function
          FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>
     <AttributeDesignator MustBePresent="false"
          Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
          AttributeId="urn:oasis:names:tc:xacml:2.0:resource:purpose"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
     <AttributeDesignator MustBePresent="false"
          Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
          AttributeId="urn:oasis:names:tc:xacml:2.0:action:purpose"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
   </Apply>
  </Apply>
</Condition>
</Rule>
```

5 Conformance

An implementation conforms to this specification by using any of the XACML attributes as defined in section 3.

Appendix A. Acknowledgments

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

Anil Saldhana
Anil Tappetla
Anne Anderson
Anthony Nadalin
Bill Parducci
Craig Forster
David Chadwick
David Staggs
Dilli Arumugam
Duane DeCouteau
Erik Rissanen
Gareth Richards
Hal Lockhart
Jan Herrmann
John Tolbert
Ludwig Seitz
Michiharu Kudo
Naomaru Itoi
Paul Tyson
Prateek Mishra
Rich Levinson
Ronald Jacobson
Seth Proctor
Sridhar Muppidi
Tim Moses
Vernon Murdoch

Appendix B. Revision History

Revision	Date	Editor	Changes Made
WD 1		Erik Rissanen	Initial update to XACML 3.0.
WD 2	28 Dec 2007	Erik Rissanen	Update to the current OASIS template.
WD 3	4 Nov 2008	Erik Rissanen	Fix typo in example
WD 4	5 Apr 2009	Erik Rissanen	Editorial cleanups. Write conformance section.
WD 05	17 Dec 2009	Erik Rissanen	Fix formatting issues Update acknowledgments
WD 06	12 Jan 2010	Erik Rissanen	Updated cross references Fixed the XML fragment so it's valid against the XACML schema. Update acknowledgments
WD 07	8 Mar 2010	Erik Rissanen	Updated cross references Fixed OASIS formatting issues
WD 08	22 Jan 2014	Erik Rissanen	Updated to current OASIS document template. Fixed broken rule in section 4.1.
WD 09	11 Mar 2014	Erik Rissanen	Fixed references.
WD 10	9 Oct 2014	Erik Rissanen	Fixed typo in hyperlink in reference to hierarchical profile. Added hyperlink to the OECD guidelines reference. Made the sample rule non-normative and updated the section to use the 3.0 combining algorithm. Updated the conformance section accordingly. Removed empty section of non-normative references.