Privacy policy profile of XACML

Committee draft 01, 16 Sep 2004

Document identifier: access_control-xacml-2.0-privacy_profile-spec-cd-01

Location: http://docs.oasis-open.org/xacml/access_control-xacml-2.0-privacy_profile-spec-cd-01.pdf

Editor:

Tim Moses, Entrust

Committee members:

Anne Anderson, Sun Microsystems
Anthony Nadalin, IBM
Bill Parducci, GlueCode Software
Daniel Engovatov, BEA Systems
Ed Coyne, Veterans Health Administration
Frank Siebenlist, Argonne National Labs
Hal Lockhart, BEA Systems
Michael McIntosh, IBM
Michiharu Kudo, IBM
Polar Humenn, Self
Ron Jacobson, Computer Associates
Seth Proctor, Sun Microsystems
Simon Godik, GlueCode Software
Steve Anderson, OpenNetwork
Tim Moses, Entrust

Abstract:

This working draft describes a profile of XACML for expressing privacy policies.

Status:

This version of the specification is an approved Committee Draft within the OASIS Access Control TC.

Access Control TC members should send comments on this specification to the xacml@lists.oasis-open.org list. Others may use the following link and complete the comment form: http://oasis-open.org/committees/comments/form.php?wg_abbrev=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 Access Control TC web page (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).

For any errata page for this specification, please refer to the Access Control TC web page (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).

Table of contents

1. Introduction (Non-normative)

1.1 Glossary

***Custodian* –** The entity to which personally-identifiable information is entrusted.

***Owner* –** The subject of personally-identifiable information.

1.2 Privacy Guidelines - Organization of Economic Cooperation and Development, 1980

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

1. within a reasonable time;

2. at a charge, if any, that is not excessive;

3. in a reasonable manner; and

4. 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.

2. Standard attributes (Normative)

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].

3. Standard rules (Normative)

3.1 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.

```
<?xml version="1.0" encoding="UTF-8"?>
<Rule xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:wd:06"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:wd:06" RuleId="
urn:oasis:names:tc:xacml:2.0:matching-purpose"
Effect="Permit">
```

```
   <Condition FunctionId="urn:oasis:names:tc:xacml:2.0:function:regexp-string-
match">
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:purpose"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
      <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:action:purpose"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
   </Condition>
</Rule>
```

4. References

[OECD] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, 1980.

[Hier] Anderson A, ed., *The XACML Profile for Hierarchical Resources,* OASIS Access Control TC, Committee Draft 01, 16 Sep 2004, http://www.oasis-open.org/committees/xacml

5. Revision history

Version	When	By whom	Changes
CD 01	16 Sep 2004	Access Control TC	Initial committee draft

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's 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 has been notified of intellectual property rights claimed in regard to some or all of the contents of this specification. For more information consult the online list of claimed rights.

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.