



1

2 Privacy policy profile of XACML

3 Committee draft 01, 16 Sep 2004

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

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

6 Editor:

7 Tim Moses, Entrust

8 Committee members:

9 Anne Anderson, Sun Microsystems

10 Anthony Nadalin, IBM

11 Bill Parducci, GlueCode Software

12 Daniel Engovatov, BEA Systems

13 Ed Coyne, Veterans Health Administration

14 Frank Siebenlist, Argonne National Labs

15 Hal Lockhart, BEA Systems

16 Michael McIntosh, IBM

17 Michiharu Kudo, IBM

18 Polar Humenn, Self

19 Ron Jacobson, Computer Associates

20 Seth Proctor, Sun Microsystems

21 Simon Godik, GlueCode Software

22 Steve Anderson, OpenNetwork

23 Tim Moses, Entrust

24 Abstract:

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

26 Status:

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

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

32 For information on whether any patents have been disclosed that may be essential to
33 implementing this specification, and any offers of patent licensing terms, please refer to the

access_control-xacml-2.0-privacy_profile-spec-cd-01

- 34 Intellectual Property Rights section of the Access Control TC web page ([http://www.oasis-](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)
35 [open.org/committees/tc_home.php?wg_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)).
- 36 For any errata page for this specification, please refer to the Access Control TC web page
37 (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).
- 38 Copyright (C) OASIS Open 2004 All Rights Reserved.

39	Table of contents	
40	1. Introduction (Non-normative)	4
41	1.1 Glossary	4
42	1.2 Privacy Guidelines - Organization of Economic Cooperation and Development, 1980	4
43	2. Standard attributes (Normative)	5
44	3. Standard rules (Normative)	5
45	3.1 Matching purpose	5
46	4. References	6
47	5. Revision history	6
48	Appendix A. Notices	7
49		

51 1. Introduction (Non-normative)

52 1.1 Glossary

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

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

55 1.2 Privacy Guidelines - Organization of Economic 56 Cooperation and Development, 1980

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

- 58 1. **Openness.** There should be limits to the collection of personal data and any such
59 data should be obtained by lawful and fair means and, where appropriate, with the
60 knowledge or consent of the data subject.
- 61 2. **Data quality principle.** Personal data should be relevant to the purposes for which
62 they are to be used, and, to the extent necessary for those purposes, should be
63 accurate, complete and kept up-to-date.
- 64 3. **Purpose specification.** The purposes for which personal data are collected should
65 be specified not later than at the time of data collection and the subsequent use
66 limited to the fulfillment of those purposes or such others as are not incompatible
67 with those purposes and as are specified on each occasion of change of purpose.
- 68 4. **Use limitation principle.** Personal data should not be disclosed, made available
69 or otherwise used for purposes other than those specified in accordance with
70 Paragraph 9 except:
- 71 (a) with the consent of the data subject; or
- 72 (b) by the authority of law.
- 73 5. **Security safeguards principle.** Personal data should be protected by reasonable
74 security safeguards against such risks as loss or unauthorized access, destruction,
75 use, modification or disclosure of data.
- 76 6. **Openness principle.** There should be a general policy of openness about
77 developments, practices and policies with respect to personal data. Means should
78 be readily available of establishing the existence and nature of personal data, and
79 the main purposes of their use, as well as the identity about usual residence of the
80 data controller.
- 81 7. **Individual participation principle.** An individual should have the right:
- 82 (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data
83 controller has data relating to him;
- 84 (b) to have communicated to him, data relating to him

- 85 1. within a reasonable time;
- 86 2. at a charge, if any, that is not excessive;
- 87 3. in a reasonable manner; and
- 88 4. in a form that is readily intelligible to him;
- 89 (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and
90 to be able to challenge such denial; and
- 91 (d) to challenge data relating to him and, if the challenge is successful, to have the data
92 erased; rectified, completed or amended.
- 93 8. **Accountability principle.** A data controller should be accountable for complying
94 with measures which give effect to the principles stated above.
- 95 This profile provides standard attributes and a standard `<Rule>` element for enforcing the 3rd and
96 4th principles, related to the purpose for which personally identifiable information is collected and
97 used.

98 2. Standard attributes (Normative)

99 This profile defines two attributes.

100 “urn:oasis:names:tc:xacml:2.0:resource:purpose”

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

105 “urn:oasis:names:tc:xacml:2.0:action:purpose”

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

109 3. Standard rules (Normative)

110 3.1 Matching purpose

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

```
115  
116   <?xml version="1.0" encoding="UTF-8"?>  
117   <Rule xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:wd:06 "  
118   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance "  
119   xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:wd:06" RuleId=" "  
120   urn:oasis:names:tc:xacml:2.0:matching-purpose "  
121   Effect="Permit">
```

```

122     <Condition FunctionId="urn:oasis:names:tc:xacml:2.0:function:regexp-string-
123 match">
124         <ResourceAttributeDesignator
125 AttributeId="urn:oasis:names:tc:xacml:2.0:resource:purpose"
126 DataType="http://www.w3.org/2001/XMLSchema#string"/>
127         <ActionAttributeDesignator
128 AttributeId="urn:oasis:names:tc:xacml:2.0:action:purpose"
129 DataType="http://www.w3.org/2001/XMLSchema#string"/>
130     </Condition>
131 </Rule>
132

```

133 4. References

- 134 **[OECD]** "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD,
135 1980.
- 136 **[Hier]** Anderson A, ed., *The XACML Profile for Hierarchical Resources*, OASIS Access Control TC,
137 Committee Draft 01, 16 Sep 2004, <http://www.oasis-open.org/committees/xacml>

138 5. Revision history

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

139

140 Appendix A. Notices

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

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

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

155 Copyright (C) OASIS Open 2004. All Rights Reserved.

156 This document and translations of it may be copied and furnished to others, and derivative works
157 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
158 published and distributed, in whole or in part, without restriction of any kind, provided that the above
159 copyright notice and this paragraph are included on all such copies and derivative works. However,
160 this document itself may not be modified in any way, such as by removing the copyright notice or
161 references to OASIS, except as needed for the purpose of developing OASIS specifications, in
162 which case the procedures for copyrights defined in the OASIS Intellectual Property Rights
163 document must be followed, or as required to translate it into languages other than English.

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

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