



1

## 2 Privacy policy profile of XACML v2.0

### 3 OASIS Standard, 1 Feb 2005

4 Document Identifier: `access_control-xacml-2.0-privacy_profile-spec-os`

5 Location: [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-privacy\\_profile-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-privacy_profile-spec-os.pdf)

6 Editor: Tim Moses, Entrust Inc. ([tim.moses@entrust.com](mailto:tim.moses@entrust.com))

#### 7 Abstract:

8 This OASIS Standard describes a profile of XACML for expressing privacy policies.

#### 9 Status:

10 This version of the specification is an approved OASIS Standard within the OASIS Access  
11 Control TC.

12 Access Control TC members should send comments on this specification to the  
13 [xacml@lists.oasis-open.org](mailto:xacml@lists.oasis-open.org) list. Others may use the following link and complete the  
14 comment form: [http://oasis-open.org/committees/comments/form.php?wg\\_abbrev=xacml](http://oasis-open.org/committees/comments/form.php?wg_abbrev=xacml).

15 For information on whether any patents have been disclosed that may be essential to  
16 implementing this specification, and any offers of patent licensing terms, please refer to the  
17 Intellectual Property Rights section of the Access Control TC web page ([http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)).

19 For any errata page for this specification, please refer to the Access Control TC web page  
20 ([http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)).

21 The non-normative errata page for this specification is located at

22 [www.oasis-open.org/committees/access-control](http://www.oasis-open.org/committees/access-control).

23 Copyright © OASIS Open 2004-2005 All Rights Reserved.

24	<b>Table of contents</b>	
25	1. Introduction (Non-normative)	3
26	1.1 Glossary	3
27	1.2 Privacy Guidelines - Organization of Economic Cooperation and Development, 1980	3
28	2. Standard attributes (Normative)	4
29	3. Standard rules (Normative)	4
30	3.1 Matching purpose	4
31	4. References	5
32	Appendix A. Acknowledgments	6
33	Appendix B. Notices	7
34		

---

## 36 1. Introduction (Non-normative)

### 37 1.1 Glossary

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

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

### 40 1.2 Privacy Guidelines - Organization of Economic 41 Cooperation and Development, 1980

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

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

- 70 1. within a reasonable time;
- 71 2. at a charge, if any, that is not excessive;
- 72 3. in a reasonable manner; and
- 73 4. in a form that is readily intelligible to him;
- 74 (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and
- 75 to be able to challenge such denial; and
- 76 (d) to challenge data relating to him and, if the challenge is successful, to have the data
- 77 erased; rectified, completed or amended.
- 78 8. **Accountability principle.** A data controller should be accountable for complying
- 79 with measures which give effect to the principles stated above.
- 80 This profile provides standard attributes and a standard `<Rule>` element for enforcing the 3<sup>rd</sup> and
- 81 4<sup>th</sup> principles, related to the purpose for which personally identifiable information is collected and
- 82 used.

---

## 83 2. Standard attributes (Normative)

84 This profile defines two attributes.

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

86 This attribute, of type "http://www.w3.org/2001/XMLSchema#string", indicates the purpose for which

87 the data resource was collected. The owner of the resource SHOULD be informed and consent to

88 the use of the resource for this purpose. The attribute value MAY be a regular expression. The

89 custodian's privacy policy SHOULD define the semantics of all available values.

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

91 This attribute, of type "http://www.w3.org/2001/XMLSchema#string", indicates the purpose for which

92 access to the data resource is requested. Action purposes MAY be organized hierarchically, in

93 which case the value MUST represent a node in the hierarchy. See [Hier].

---

## 94 3. Standard rules (Normative)

### 95 3.1 Matching purpose

96 This rule MUST be used with the "urn:oasis:names:tc:xacml:2.0:rule-combining-algorithm:deny-

97 overrides" rule-combining algorithm. It stipulates that access SHALL be denied unless the purpose

98 for which access is requested matches, by regular-expression match, the purpose for which the

99 data resource was collected.

100  
101  
102  
103  
104  
105

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

```
106 Effect="Permit">
107   <Condition FunctionId="urn:oasis:names:tc:xacml:2.0:function:regex-string-
108   match">
109     <ResourceAttributeDesignator
110     AttributeId="urn:oasis:names:tc:xacml:2.0:resource:purpose"
111     DataType="http://www.w3.org/2001/XMLSchema#string"/>
112     <ActionAttributeDesignator
113     AttributeId="urn:oasis:names:tc:xacml:2.0:action:purpose"
114     DataType="http://www.w3.org/2001/XMLSchema#string"/>
115   </Condition>
116 </Rule>
117
```

---

## 118 4. References

- 119 **[OECD]** "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD,  
120 1980.
- 121 **[Hier]** Anderson A, ed., *The XACML Profile for Hierarchical Resources*, OASIS Access Control TC,  
122 OASIS Standard, 1 Feb 2005, <http://www.oasis-open.org/committees/xacml>

---

## 123 Appendix A. Acknowledgments

124 The following individuals contributed to the development of the specification:

125 Anne Anderson  
126 Anthony Nadalin  
127 Bill Parducci  
128 Daniel Engovatov  
129 Don Flinn  
130 Ed Coyne  
131 Ernesto Damiani  
132 Frank Siebenlist  
133 Gerald Brose  
134 Hal Lockhart  
135 Haruyuki Kawabe  
136 James MacLean  
137 John Merrells  
138 Ken Yagen  
139 Konstantin Beznosov  
140 Michiharu Kudo  
141 Michael McIntosh  
142 Pierangela Samarati  
143 Pirasenna Velandai Thiyagarajan  
144 Polar Humenn  
145 Rebekah Metz  
146 Ron Jacobson  
147 Satoshi Hada  
148 Sekhar Vajjhala  
149 Seth Proctor  
150 Simon Godik  
151 Steve Anderson  
152 Steve Crocker  
153 Suresh Damodaran  
154 Tim Moses  
155 Von Welch  
156 Seth Proctor  
157 Simon Godik  
158 Steve Anderson  
159 Steve Crocker  
160 Tim Moses

---

161

## Appendix B. Notices

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

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

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

### 176 **Copyright (C) OASIS Open 2004, 2005. All Rights Reserved.**

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

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

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