



2 XML Digital Signature profile of
3 XACML v2.0

4 OASIS Standard, 1 February 2005

5 **Document identifier:**

6 access_control-xacml-2.0-dsig-profile-spec-os

7 **Location:**

8 http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-dsig-profile-spec-os.pdf

9 **Editor:**

10 Anne Anderson, Sun Microsystems <anne.anderson@sun.com>

11 **Abstract:**

12 This specification profiles use of the W3C XML-Signature Syntax and Processing
13 Standard in providing authentication and integrity protection for XACML schema
14 instances.

15 **Status:**

16 This version of the specification is an approved OASIS Standard.

17 Access Control TC members should send comments on this specification to the
18 xacml@lists.oasis-open.org list. Others should use the comment form at [http://oasis-](http://oasis-open.org/committees/comments/form.php?wg_abbrev=xacml)
19 [open.org/committees/comments/form.php?wg_abbrev=xacml](http://oasis-open.org/committees/comments/form.php?wg_abbrev=xacml).

20 For information on whether any patents have been disclosed that may be essential to
21 implementing this specification, and any offers of patent licensing terms, please refer to
22 the Intellectual Property Rights section of the Access Control TC web page
23 (<http://www.oasis-open.org/committees/xacml/ipr.php>).

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

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

Table of Contents

27	1 Introduction (non-normative).....	3
28	1.1 Terminology.....	3
29	2 XML Digital Signature profile of XACML.....	4
30	2.1 Use of SAML.....	4
31	2.2 Canonicalization.....	4
32	2.3 Signing schemas.....	5
33	3 References	6
34	Appendix A. Acknowledgments.....	7
35	Appendix B. Notices.....	8

36 1 Introduction (non-normative)

37 This document provides a profile for use of the W3C XML-Signature Syntax and Processing
38 Standard in providing authentication and integrity protection for OASIS eXtensible Access
39 Control Markup Language [XACML] schema instances. Sections 9.2.1 Authentication and 9.2.4
40 Policy integrity in [XACML] describe requirements and considerations for such authentication
41 and integrity protection.

42 A digital signature is useful for authentication and integrity protection only if the signed
43 information includes a specification of the identity of the signer and a specification of the period
44 during which the signed data object is to be considered valid. XACML itself does not define the
45 format for such information, as XACML is intended to use other standards for functions other
46 than the actual specification and evaluation of access control policies, requests, and responses.

47 One appropriate format that has been defined elsewhere is [SAML].. A profile for the use of
48 SAML with XACML schema instances is available in [XACML-SAML]. This profile therefore
49 RECOMMENDS use of XACML schema instances in SAML Assertions, Requests, and
50 Responses, which MAY then be digitally signed as specified in the SAML specification.

51 This profile also notes various canonicalization issues that must be resolved in order for signed
52 documents to be verified by a relying party.

53 This profile specification assumes that the reader is familiar with the concept of a digital
54 signature, with the W3C XML-Signature Syntax and Processing Standard, and with XACML.

55 1.1 Terminology

56 *(This section is not normative.)*

57 The key words MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD
58 NOT, RECOMMENDED, MAY, and OPTIONAL in this profile are to be interpreted as described
59 in [RFC2119].

60 **data object** – used in this profile to refer to a digital object that is being signed. A data object
61 could be an XACML PolicySet, Policy, Request context, Response context, or any associated
62 schemas. A data object is referenced inside an [XMLDSIG] <Reference> element using a URI
63 as defined by [RFC2396].

64 2 XML Digital Signature profile of XACML

65 2.1 Use of SAML

66 *(This section is normative)*

67 This Profile RECOMMENDS use of XACML schema instances embedded in SAML Assertions,
68 Requests, and Responses as described in [XACML-SAML]. Such SAML objects SHALL be
69 digitally signed as described in *Section 5: SAML and XML Signature Syntax and Processing of*
70 [SAML].

71 2.2 Canonicalization

72 In order for a digital signature to be verified by a relying party, the byte stream that was signed
73 MUST be identical to the byte stream that is verified. To ensure this, the XML document being
74 signed MUST be *canonicalized*. *Section 5: SAML and XML Signature Syntax and Processing of*
75 [SAML] specifies use of Exclusive Canonicalization [ExclC14N].

76 2.2.1 Namespace elements in XACML data objects

77 Any XACML **data object** that is to be signed MUST specify all namespace elements used in the
78 **data object**. If this is not done, then the **data object** will attract namespace definitions from
79 ancestors of the **data object** that may differ from one envelope to another.

80 When [ExclC14N] is used as the **canonicalization** or transform method, then the namespace of
81 XACML schemas used by elements in an XACML **data object** MUST be bound to prefixes and
82 included in the *InclusiveNamespacesPrefixList* parameter to [ExclC14N].

83 2.2.2 Additional canonicalization considerations

84 Additional transformations on the XACML data object must usually be performed in order to
85 ensure that the data object signed will match the data object that is verified. Some of these
86 transformations are listed here, but this Profile does not attempt to specify algorithms for
87 performing these.

88 If an XACML **data object** includes data elements that may be represented in more than one
89 form (such as (TRUE, FALSE), (1,0), (true,false)), then a Transform method MUST be defined
90 and specified for normalizing those data elements.

91 This Profile RECOMMENDS applying the following canonicalizations to values of the
92 corresponding datatypes, whether occurring in XML attribute values or in XACML Attributes.

- 93 1. Where a canonical representation for an XACML-defined datatype is defined in
94 <http://www.w3.org/2001/XMLSchema>, then the value of the datatype MUST be put into the
95 canonical form specified in <http://www.w3.org/2001/XMLSchema>. This includes boolean
96 {"true", "false"}, double, dateTime, time, date, and hexBinary (upper-case).
- 97 2. <http://www.w3.org/2001/XMLSchema#anyURI> - use the canonical form defined in [RFC2396]

- 98 3. <http://www.w3.org/2001/XMLSchema#base64Binary> - remove all line breaks and white
99 space. Remove all characters following the first sequence of “=” characters. The *Base64*
100 *Transform* (identifier: <http://www.w3.org/TR/xmlsig-core/#sec-Base-64>) MAY be useful in
101 performing this canonicalization.
- 102 4. <urn:oasis:names:tc:xacml:1.0:data-type:x500Name> - first normalize according to [RFC2253].
103 If any RDN contains multiple attributeTypeAndValue pairs, re-order the AttributeValuePairs in
104 that RDN in ascending order when compared as octet strings (described in Section 11.6 “Set-
105 of components” of [X.690]).
- 106 5. <urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name> - normalize the domain-part of the name
107 to lower case.
- 108 6. XPath expression – apply [XPath2Filt] to put the XPath expression into canonical form.
- 109 *Schema Centric XML Canonicalization Version 1.0* [ScC14N] describes many canonicalization
110 issues for XML documents that should be addressed.

111 2.3 Signing schemas

112 The parsing of any XACML **data object** depends on having an accurate copy of all schemas on
113 which the XACML **data object** depends. Note that the inclusion of a schema URI in the XACML
114 schema instance attributes does not guarantee that an accurate copy of the schema will be
115 used: an attacker may substitute a bogus schema that contains the correct identifier.

116 **Signatures** can help protect against substitution or modification of the schemas on which an
117 XACML **data object** depends. Use of **signatures** for this purpose are described in this section.

118 In most cases, a **data object** signer SHOULD include a <Reference> element for each schema
119 on which the XACML **data object** depends in the <SignedInfo> element that contains the
120 <Reference> to or including the XACML **data object** itself.

121 In some cases, the **data object** signer knows that all PDPs that will evaluate a given XACML
122 **data object** will have accurate copies of certain schemas needed to parse the **data object**, and
123 does not want to force the PDP to verify the message digest for such schemas. In these cases
124 the **data object** signer MAY omit <Reference> elements for any schema whose verification is
125 not needed.

126 3 References

- 127 [ExcIC14N] J. Boyer et al., *Exclusive Canonicalization Version 1.0*, 18 January 2002,
128 World Wide Web Consortium, <http://www.w3.org/TR/xml-exc-c14n/>.
- 129 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
130 IETF RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.
- 131 [RFC2253] M. Wahl, et al., *Lightweight Directory Access Protocol (v3): UTF-8
132 String Representation of Distinguished Names*, IETF RFC 2253,
133 September 1997, <http://www.ietf.org/rfc/rfc2253.txt>.
- 134 [RFC2396] T. Berners-Lee, et al., *Uniform Resource Identifiers (URI): Generic
135 Syntax*, August 1998, <http://ftp://ftp.isi.edu/in-notes/rfc2396.txt>.
- 136 [SAML] S. Cantor, et al., eds., *Assertions and Protocols for the OASIS Security
137 Assertion Markup Language (SAML) V2.0*, [http://www.oasis-
138 open.org/committees/documents.php?wg_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security).
- 139 [ScC14N] S. Aissi, M. Hondo, eds., *Schema Centric XML Canonicalization,
140 Version 1.0*, 20 May 2003,
141 <http://uddi.org/pubs/SchemaCentricCanonicalization.htm>.
- 142 [XACML] T. Moses, ed., *OASIS eXtensible Access Control Markup Language
143 (XACML) Version 2.0*, OASIS Standard, 1 February 2005,
144 [http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-
145 spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf).
- 146 [XACML-SAML] A. Anderson, H. Lockhart, eds., *SAML 2.0 profile of XACML v2.0*,
147 OASIS Standard, 1 February 2005, [http://docs.oasis-
148 open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf).
- 149 [XMLDSIG] D. Eastlake, et al., *W3C XML-Signature Syntax and Processing*, W3C
150 Recommendation, 12 February 2002, [http://www.w3.org/TR/xmlldsig-
151 core](http://www.w3.org/TR/xmlldsig-core).
- 152 [XPath2Filt] J. Boyer, M. Hughes, J. Reagle, editors, *XML-Signature XPath Filter 2.0*,
153 8 November 2002 <http://www.w3.org/TR/xmlldsig-filter2/>.
- 154 [X.690] ITU-T Recommendation X.690 Information Technology – Open Systems
155 Interconnection - Procedures for the operation of OSI Registration
156 Authorities: General procedures, 1992.

157 Appendix A. Acknowledgments

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

159 Anne Anderson
160 Anthony Nadalin
161 Bill Parducci
162 Daniel Engovatov
163 Don Flinn
164 Ed Coyne
165 Ernesto Damiani
166 Frank Siebenlist
167 Gerald Brose
168 Hal Lockhart
169 Haruyuki Kawabe
170 James MacLean
171 John Merrells
172 Ken Yagen
173 Konstantin Beznosov
174 Michiharu Kudo
175 Michael McIntosh
176 Pierangela Samarati
177 Pirasenna Velandai Thiyagarajan
178 Polar Humenn
179 Rebekah Metz
180 Ron Jacobson
181 Satoshi Hada
182 Sekhar Vajjhala
183 Seth Proctor
184 Simon Godik
185 Steve Anderson
186 Steve Crocker
187 Suresh Damodaran
188 Tim Moses
189 Von Welch

190 Appendix B. Notices

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

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

203 **Copyright © OASIS Open 2004-2005. All Rights Reserved.**

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

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

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