eXtensible Access Control Markup Language (XACML) Media Type
draft-sinnema-xacml-media-type-02

Abstract

   This specification registers an XML-based media type for the
   eXtensible Access Control Markup Language (XACML).

Note to Readers

   This draft should be discussed on the apps-discuss mailing list [1].

   Online access to all versions and files is available on github [2].

Status of this Memo

Copyright Notice

   include Simplified BSD License text as described in Section 4.e of
   the Trust Legal Provisions and are provided without warranty as
   described in the Simplified BSD License.

Table of Contents

1. Introduction

   The eXtensible Access Control Markup Language (XACML) [XACML-3]
   defines an architecture and a language for access control
   (authorization). The language consists of requests, responses, and
   policies. Clients sends a request to a server to query whether a
   given action should be allowed. The server evaluates the request
   against the available policies and returns a reponse. The policies
   implement the organization's access control requirements.

2. XACML Media Type

   This specification registers an XML-based media type for the
   eXtensible Access Control Markup Language (XACML) that will be
   registered with the Internet Assigned Numbers Authority (IANA)
   following the "Media Type Specifications and Registration Procedures"
   [RFC6838]. The XACML media type represents an XACML request,
   response, or policy in the XML-based format defined by the core XACML
   specification [XACML-3].

3. XACML Media Type application/xacml+xml

   This specification requests the registration of an XML-based media
   type for the eXtensible Access Control Markup Language (XACML).

3.1. Media Type Name

   application

3.2. Subtype Name

   xacml+xml

3.3. Required Parameters

3.4. Optional Parameters

   charset: The charset parameter is the same as the charset parameter
   of application/xml [RFC3023].

   version: The version parameter indicates the version of the XACML
   specification. It can be used for content negotiation when dealing
   with clients and servers that support multiple XACML versions. Its
   range is the range of published XACML versions. As of this writing

that is: 1.0 [XACML-1], 1.1 [XACML-1.1], 2.0 [XACML-2], and 3.0
[XACML-3]. These and future version identifiers consist of a series
of non-negative decimal numbers with no leading zeros separated by
dots, where the first decimal must be positive. If this parameter is
not specified by the client, the server is free to return any version
it deems fit. If a client cannot or does not want to deal with that,
it should explicitly specify a version.

3.5. Encoding Considerations

Same as for application/xml [RFC3023].

3.6. Security Considerations

Per their specification, application/xacml+xml typed objects do not
contain executable content. However, these objects are XML-based,
and thus they have all of the general security considerations
presented in section 10 of RFC 3023 [RFC3023].

XACML [XACML-3] contains information whose integrity and authenticity
is important - identity provider and service provider public keys and
endpoint addresses, for example. Sections 9.2.1 Authentication and
9.2.4 Policy integrity in XACML [XACML-3] describe requirements and
considerations for such authentication and integrity protection.

To counter potential issues, the publisher may sign application/
xacml+xml typed objects. Any such signature should be verified by
the recipient of the data - both as a valid signature, and as being
the signature of the publisher. The XACML v3.0 XML Digital Signature
Profile [XACML-3-DSig] describes how to use XML-based digital
signatures with XACML.

Additionally, various of the possible publication protocols, for
example HTTPS, offer means for ensuring the authenticity of the
publishing party and for protecting the policy in transit.

For a more detailed discussion of XACML policy and its security
considerations, please see XACML 3.0 [XACML-3] and the associated XML
Digital Signature Profile [XACML-3-DSig].

3.7. Interoperability Considerations

Different versions of XACML use different XML namespace URIS:

o 1.0 & 1.1 use the urn:oasis:names:tc:xacml:1.0:policy XML
   namespace URI for policies, and the
   urn:oasis:names:tc:xacml:1.0:context XML namespace URI for
   requests and responses

o 2.0 uses the urn:oasis:names:tc:xacml:2.0:policy XML namespace URI
   for policies, and the urn:oasis:names:tc:xacml:2.0:context XML
   namespace URI for requests and responses

o 3.0 uses the urn:oasis:names:tc:xacml:3.0:core:schema:wd-17 XML
   namespace URI for policies, requests, and responses

Signed XACML has a wrapping SAML 2.0 assertion [SAML-2], which uses
the urn:oasis:names:tc:SAML:2.0:assertion namespace URI.
Interoperability with SAML is defined by the SAML 2.0 Profile of
XACML [XACML-3-SAML] for all versions of XACML.

3.8. Applications which use this media type

Potentially any application implementing or using XACML, as well as
those applications implementing or using specifications based on
XACML.

3.9. Magic number(s)

In general, the same as for application/xml [RFC3023]. In
particular, the XML document element of the returned object will be
one of xacml:Policy, xacml:PolicySet, context:Request, or context:
Response. The xacml and context prefixes differ for the various
versions of XACML as follows:

o 1.0 & 1.1: The xacml prefix maps to
   urn:oasis:names:tc:xacml:1.0:policy, the context prefix maps to
   urn:oasis:names:tc:xacml:1.0:context

o 2.0: The xacml prefix maps to urn:oasis:names:tc:xacml:2.0:policy,
   the context prefix maps to urn:oasis:names:tc:xacml:2.0:context

o 3.0: Both the xacml and context prefixes map to the namespace URI
   urn:oasis:names:tc:xacml:3.0:core:schema:wd-17

For signed XACML [XACML-3-DSig], the XML document element is saml:
Assertion, where the saml prefix maps to the SAML 2.0 namespace URI
urn:oasis:names:tc:SAML:2.0:assertion [SAML-2]

3.10. File extension(s)

3.11. Macintosh File Type Code(s)

3.12. Person & email address to contact for further information

   This registration is made on behalf of the OASIS eXtensible Access
   Control Markup Language Technical Committee (XACMLTC). Please refer
   to the XACMLTC website for current information on committee
   chairperson(s) and their contact addresses:
   http://www.oasis-open.org/committees/xacml/. Committee members
   should submit comments and potential errata to the
   xacml@lists.oasis-open.org list. Others should submit them by
   filling out the web form located at http://www.oasis-open.org/
   committees/comments/form.php?wg_abbrev=xacml.

   Additionally, the XACML developer community email distribution list,
   xacml-dev@lists.oasis-open.org, may be employed to discuss usage of
   the application/xacml+xml MIME media type. The xacml-dev mailing
   list is publicly archived here:
   http://www.oasis-open.org/archives/xacml-dev/. To post to the xacml-
   dev mailing list, one must subscribe to it. To subscribe, visit the
   OASIS mailing list page at http://www.oasis-open.org/mlmanage/.

3.13. Intended Usage

   Common

3.14. Author/Change Controller

   The XACML specification sets are a work product of the OASIS
   eXtensible Access Control Markup Language Technical Committee
   (XACMLTC). OASIS and the XACMLTC have change control over the XACML
   specification sets.

4. Change Log

   Note to RFC Editor: Please remove this section before publication.

4.1. From -01 to -02

   o Added new introduction text.

   o Improved definition of version numbers and their handling.

4.2. From -00 to -01

   o Added new introduction text.

   o Changed reference from RFC 4288 to RFC 6838 (updated RFC for media
      type registrations).

4.3. Versions prior to I-D -00

Prior to being published as a I-D document, this document was
published and revised as an OASIS document with the following
versions:

o 2012-02-29 (WD01): Initial revision with one media type.

o 2012-04-23 (WD02): Added JSON media type.

o 2012-04-24 (WD03): Fixed layout, typos, and references. Better
   defined the allowable range of values for the version parameter.

5. Normative References

[RFC3023] Murata, M., St. Laurent, S., and D. Kohn, "XML Media
           Types", RFC 3023, January 2001.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type
           Specifications and Registration Procedures", BCP 13,
           RFC 6838, January 2013.

[SAML-2]   Organization for the Advancement of Structured Information
           Standards, "Security Assertion Markup Language (SAML)
           Version 2.0. OASIS Standard", March 2005, <http://
           docs.oasis-open.org/security/saml/v2.0/
           saml-core-2.0-os.pdf>.

[XACML-1] Organization for the Advancement of Structured Information
           Standards, "eXtensible Access Control Markup Language
           (XACML) Version 1.0. OASIS Standard", February 2003, <http
           ://www.oasis-open.org/committees/download.php/2406/
           oasis-xacml-1.0.pdf>.

[XACML-1.1]
           Organization for the Advancement of Structured Information
           Standards, "eXtensible Access Control Markup Language
           (XACML) Version 1.1. OASIS Committee Specification",
           August 2003, <http://www.oasis-open.org/committees/xacml/
           repository/cs-xacml-specification-1.1.pdf>.

[XACML-2] Organization for the Advancement of Structured Information
           Standards, "eXtensible Access Control Markup Language
           (XACML) Version 2.0. OASIS Standard", February 2005, <http
           ://docs.oasis-open.org/xacml/2.0/
           access_control-xacml-2.0-core-spec-os.pdf>.

   [XACML-3] Organization for the Advancement of Structured Information
              Standards, "eXtensible Access Control Markup Language
              (XACML) Version 3.0. OASIS Committee Specification 01",
              August 2010, <http://docs.oasis-open.org/xacml/3.0/
              xacml-3.0-core-spec-cs-01-en.pdf>.

   [XACML-3-DSig]
              Organization for the Advancement of Structured Information
              Standards, "XACML v3.0 XML Digital Signature Profile
              Version 1.0. OASIS Committee Specification 01",
              August 2010, <http://docs.oasis-open.org/xacml/3.0/
              xacml-3.0-dsig-v1-spec-cs-01-en.pdf>.

   [XACML-3-SAML]
              Organization for the Advancement of Structured Information
              Standards, "SAML 2.0 Profile of XACML, Version 2.0. OASIS
              Committee Specification 01", August 2010, <http://
              docs.oasis-open.org/xacml/3.0/
              xacml-profile-saml2.0-v2-spec-cs-01-en.pdf>.

   [1]   <https://www.ietf.org/mailman/listinfo/apps-discuss>

   [2]   <https://github.com/dret/I-D/tree/master/xacml-media-type>

Appendix A. Acknowledgements

   The following individuals have participated in the creation of this
   specification and are gratefully acknowledged: Erik Rissanen
   (Axiomatics) and Jonathan Robie (EMC).

Authors' Addresses

   Remon Sinnema
   EMC Corporation

   Email: remon.sinnema@emc.com
   URI: http://securesoftwaredev.com/

Erik Wilde
EMC Corporation
6801 Koll Center Parkway
Pleasanton, CA 94566
U.S.A.

Phone: +1-925-6006244
Email: erik.wilde@emc.com
URI: http://dret.net/netdret/