Independent Submission
Request for Comments: 7061
Category: Informational
ISSN: 2070-1721

R. Sinnema
E. Wilde
EMC Corporation

November 2013

eXtensible Access Control Markup Language (XACML) XML Media Type

Abstract

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

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7061.

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 send 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 response. The policies implement the organization’s access control requirements.

2. IANA Considerations

This specification details the registry of an XML-based media type for the eXtensible Access Control Markup Language (XACML) that has been 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].

2.1. XACML Media Type application/xacml+xml

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

Media Type Name: application

Subtype Name: xacml+xml

Required Parameters: none

Optional Parameters:

charset: The charset parameter is the same as the charset parameter of application/xml [RFC3023], including the same default (see Section 3.2 of RFC 3023).

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 must follow the Organization for the Advancement of Structured Information Standards (OASIS) patterns for versions [OASIS-Version]. 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.

Encoding Considerations: Same as for application/xml [RFC3023].

Security Considerations:

Per their specification, objects of type application/xacml+xml 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 about 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 objects of type application/xacml+xml. Any such signature should be verified -- both as a valid signature and as being the signature of the publisher -- by the recipient of the data. The XACML v3.0 XML Digital Signature Profile [XACML-3-DSig] describes how to use XML-based digital signatures with XACML.

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

Interoperability Considerations: Different versions of XACML use different XML namespace URIs:

* 1.0 and 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

* 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

* 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 Security Assertion Markup Language (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.

Applications That Use This Media Type:

Potentially, any application implementing or using XACML, as well as those applications implementing or using specifications based on XACML. In particular, applications using the Representational State Transfer (REST) Profile [XACML-REST] can benefit from this media type.

Magic Number(s):

In general, this is 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 namespace prefixes bind to the respective namespace URIs for the various versions of XACML as follows:

* 1.0 and 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

* 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

* 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].

File Extension(s): none

Macintosh File Type Code(s): none

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 errors 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/.

Intended Usage: common

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.

3. Security Considerations

The security considerations for this specification are described in Section 2.1 of the media type registration.

4. Normative References

[OASIS-Version] Organization for the Advancement of Structured Information Standards, "OASIS Naming Directives Version 1.3", December 2012, <http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#Version>.

[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, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", 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 Standard, January 2013, <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-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>.

[XACML-REST]
Organization for the Advancement of Structured Information Standards, "REST Profile of XACML v3.0 Version 1.0", OASIS Committee Specification 01, April 2013, <http://docs.oasis-open.org/xacml/xacml-rest/v1.0/xacml-rest-v1.0.pdf>.

Appendix A. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged: Oscar Koeroo (Nikhef), 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
USA

Phone: +1-925-600-6244
EMail: erik.wilde@emc.com
URI: http://dret.net/netdret/