



# REST Profile of XACML v3.0 Version 1.0

## Committee Specification Draft 01

15 November 2012

### Specification URIs

#### This version:

<http://docs.oasis-open.org/xacml/xacml-rest/v1.0/csd01/xacml-rest-v1.0-csd01.doc> (Authoritative)  
<http://docs.oasis-open.org/xacml/xacml-rest/v1.0/csd01/xacml-rest-v1.0-csd01.html>  
<http://docs.oasis-open.org/xacml/xacml-rest/v1.0/csd01/xacml-rest-v1.0-csd01.pdf>

#### Previous version:

N/A

#### Latest version:

<http://docs.oasis-open.org/xacml/xacml-rest/v1.0/xacml-rest-v1.0.doc> (Authoritative)  
<http://docs.oasis-open.org/xacml/xacml-rest/v1.0/xacml-rest-v1.0.html>  
<http://docs.oasis-open.org/xacml/xacml-rest/v1.0/xacml-rest-v1.0.pdf>

#### Technical Committee:

OASIS eXtensible Access Control Markup Language (XACML) TC

#### Chairs:

Hal Lockhart ([hal.lockhart@oracle.com](mailto:hal.lockhart@oracle.com)), Oracle  
Bill Parducci ([bill@parducci.net](mailto:bill@parducci.net)), Individual

#### Editor:

Rémon Sinnema ([remon.sinnema@emc.com](mailto:remon.sinnema@emc.com)), EMC

#### Related work:

This specification is related to:

- *eXtensible Access Control Markup Language (XACML) Version 3.0*. Latest version.  
<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html>.

#### Abstract:

This specification defines a profile for the use of XACML in a RESTful architecture.

#### Status:

This document was last revised or approved by the OASIS eXtensible Access Control Markup Language (XACML) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/xacml/>.

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

#### Citation format:

When referencing this specification the following citation format should be used:

**[XACML-REST-v1.0]**

*REST Profile of XACML v3.0 Version 1.0.* 15 November 2012. OASIS Committee Specification  
Draft 01. <http://docs.oasis-open.org/xacml/xacml-rest/v1.0/csd01/xacml-rest-v1.0-csd01.html>.

---

## Notices

Copyright © OASIS Open 2012. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

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

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

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

---

# Table of Contents

|             |  |    |
|-------------|--|----|
| 1           | Introduction .....                       | 5  |
| 1.1         | Terminology .....                        | 5  |
| 1.2         | Glossary .....                           | 5  |
| 1.3         | Normative References .....               | 5  |
| 1.4         | Non-Normative References .....           | 6  |
| 1.5         | Rationale .....                          | 7  |
| 1.5.1       | Externalization of Access Control .....  | 7  |
| 1.5.2       | Cloud Computing .....                    | 7  |
| 1.5.3       | REST .....                               | 7  |
| 1.5.4       | RESTful Authorization as a Service ..... | 8  |
| 1.6         | Use Cases .....                          | 8  |
| 1.6.1       | PEP ↔ PDP .....                          | 8  |
| 2           | RESTful Services .....                   | 9  |
| 2.1         | Network Transport .....                  | 9  |
| 2.2         | Resources .....                          | 9  |
| 2.2.1       | Entry Point .....                        | 9  |
| 2.2.2       | Policy Decision Point .....              | 9  |
| 2.3         | Representations .....                    | 10 |
| 2.3.1       | Linking .....                            | 10 |
| 2.3.2       | Entry Point .....                        | 11 |
| 2.4         | Examples .....                           | 11 |
| 2.4.1       | Obtain an Access Decision .....          | 11 |
| 3           | Security Considerations .....            | 12 |
| 3.1         | Network Transport .....                  | 12 |
| 3.2         | Authentication .....                     | 12 |
| 3.3         | Authorization .....                      | 12 |
| 3.4         | Non-Repudiation .....                    | 12 |
| 4           | Conformance .....                        | 13 |
| 4.1         | Conformance Clauses .....                | 13 |
| 4.2         | Test Assertions .....                    | 13 |
| 4.2.1       | Network Transport .....                  | 13 |
| 4.2.2       | Entry Point .....                        | 13 |
| 4.2.3       | Policy Decision Point .....              | 14 |
| Appendix A. | Acknowledgments .....                    | 16 |
| Appendix B. | Revision History .....                   | 17 |

---

# 1 Introduction

## {Non-normative}

This specification defines a profile for the use of the OASIS eXtensible Access Control Markup Language (XACML), versions 3.0 [XACMLv3] and earlier. Use of this profile requires no changes or extensions to the XACML standard.

This specification begins with a non-normative discussion of the topics and terms of interest in this profile. The normative section of the specification describes the details of web services that conforming implementations must support.

This specification assumes the reader is somewhat familiar with XACML. A brief overview of XACML is available in [XACMLIntro].

## 1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

## 1.2 Glossary

### Client

The agent that initiates *requests* to a *server*.

### Representation

A sequence of bytes, in a given format, that represents a *resource* in some way.

### Request

The HTTP request message sent from the *client* to the *server* [HTTP]. Note that this is not the same concept as a XACML request [XACMLv3].

### Resource

A service that is offered by the *server* [REST]. This can be static, like a document, or dynamic, like a search. Note that this is not the same concept as a XACML resource [XACMLv3].

### Response

The HTTP response message returned from the *server* to the *client* [HTTP]. Note that this is not the same concept as a XACML response [XACMLv3].

### Server

The agent that handles *requests* from a *client*.

## 1.3 Normative References

- |           |  |
|-----------|--|
| [Atom]    | <i>The Atom Syndication Format</i> . December 2005. IETF RFC 4287.<br><a href="http://tools.ietf.org/html/rfc4287">http://tools.ietf.org/html/rfc4287</a>                        |
| [HTTP]    | <i>Hypertext Transfer Protocol</i> . June 1999. IETF RFC 2616.<br><a href="http://tools.ietf.org/html/rfc2616">http://tools.ietf.org/html/rfc2616</a>                            |
| [RFC2119] | <i>Key words for use in RFCs to Indicate Requirement Levels</i> . March 1997. IETF RFC 2119. <a href="http://tools.ietf.org/html/rfc2119">http://tools.ietf.org/html/rfc2119</a> |

- [TAG]** *Test Assertions Part 1 - Test Assertions Model Version 1.0*. 30 November 2011. OASIS Committee Specification 02. <http://docs.oasis-open.org/tag/model/v1.0/cs02/testassertionsmodel-1.0-cs02.pdf>
- [URI]** *Uniform Resource Identifier (URI): Generic Syntax*. January 2005. IETF RFC 3986. <http://tools.ietf.org/html/rfc3986>
- [WebLink]** *Web Linking*. October 2010. IETF RFC 4287. <http://tools.ietf.org/html/rfc5988>
- [XACMLMedia]** *eXtensible Access Control Markup Language (XACML) Media Type*. 14 September 2012. IETF Draft 00. <http://tools.ietf.org/html/draft-sinnema-xacml-media-type-00>
- [XACMLv3]** *eXtensible Access Control Markup Language (XACML) Version 3.0*. 8 August 2012. OASIS Committee Specification 02. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs02-en.pdf>

## 1.4 Non-Normative References

- [Admin]** *XACML v3.0 Administration and Delegation Profile Version 1.0*. 10 August 2010. OASIS Committee Specification 01. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-administration-v1-spec-en.pdf>
- [Cloud]** *The NIST Definition of Cloud Computing*. September 2011. National Institute of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- [HomeDocument]** *Home Documents for HTTP APIs*. May 2012. Internet-Draft. <http://tools.ietf.org/html/draft-nottingham-json-home-00>
- [HTTPAuthN]** HTTP Authentication: Basic and Digest Access Authentication. June 1999. IETF RFC 2617. <http://tools.ietf.org/html/rfc2617>
- [HTTPS]** *HTTP over TLS*. May 2000. IETF RFC 2818. <http://tools.ietf.org/html/rfc2818>
- [Media]** *MIME Media Types*. <http://www.iana.org/assignments/media-types/index.html>
- [OpenID]** *OpenID Authentication 2.0*. 5 December 2007. [http://openid.net/specs/openid-authentication-2\\_0.html](http://openid.net/specs/openid-authentication-2_0.html)
- [REST]** *Roy Fielding, Architectural Styles and the Design of Network-based Software Architectures*. 2000. [http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding\\_dissertation.pdf](http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf)
- [SAMLv2]** *Security Assertion Markup Language (SAML) Version 2.0*. 15 March 2005. OASIS Standard. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [SAML4XACML]** *SAML 2.0 Profile of XACML, Version 2.0*. 10 August 2010. OASIS Committee Specification 01. <http://docs.oasis-open.org/xacml/3.0/xacml-profile-saml2.0-v2-spec-cs-01-en.pdf>

- [SASL] *Simple Authentication and Security Layer (SASL)*. June 2006. IETF RFC 4422. <http://tools.ietf.org/html/rfc4422>
- [SecaaS] *Security as a Service: Defined Categories of Service*, October 10 2011. [https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS\\_V1\\_0.pdf](https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf)
- [XACMLIntro] *A Brief Introduction to XACML*. 14 March 2003, [http://www.oasis-open.org/committees/download.php/2713/Brief\\_Introduction\\_to\\_XACML.html](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)

## 1.5 Rationale

### 1.5.1 Externalization of Access Control

XACML [XACMLIntro] can be used for controlling access within a single application. This removes hard-coded security constraints from the application code, making it easier to change them. It also makes it possible to use a standard Policy Decision Point (PDP), so that organizations can make a proper make-or-buy decision. For virtually all organizations, authorization is not their core business, so being able to use an off-the-shelf product is appealing.

Although these are substantial benefits, XACML really shines when authorization is completely externalized from the application. Policies can then be reused across many applications, each using the same PDP. This leads to greater consistency of access control rules and improved efficiency in maintaining them.

### 1.5.2 Cloud Computing

Once access control policies are externalized from the application, the PDP can become a service to be shared in a cloud computing scenario.

The National Institute of Standards and Technology (NIST) defines cloud computing as “*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*” [Cloud].

Applying the ideas of cloud computing to access control leads to *Authorization as a Service* (AZaaS). The Cloud Security Alliance sees this as part of the Identity and Access Management category of service that they distinguish in the Security as a Service field [SecaaS]. Note that AZaaS requires a much heavier load on **servers** than Authentication as a Service, since authentication happens only once for a user session, while authorization must occur on every user action.

### 1.5.3 REST

In cloud computing, services are shared and must therefore be accessed over a computer network. Cloud infrastructure will thus by definition have a network-addressable API. Such an API can be built on RESTful principles.

*REpresentational State Transfer* (REST) is a system of architectural constraints that govern the interaction between a **client** and a **server** [REST]. In cloud computing, the **client** is the cloud service consumer, and the **server** is the cloud service itself. The constraints that REST adds to a **client-server** system are:

1. **Statelessness:** Each **request** from **client** to **server** must contain all of the information necessary to understand the **request**, and cannot take advantage of any stored context on the **server**. It improves visibility, reliability and scalability.
2. **Cache:** Data within a **response** to a **request** must be implicitly or explicitly labeled as cacheable or non-cacheable. It improves efficiency and scalability.
3. **Uniform interface:** **Client** and **server** interact through a generalized interface. It improves visibility, simplicity and evolvability, at the expense of efficiency. This is the distinguishing feature of REST. The constraints on the generalized interface are:

- i. **Identification of resources:** The key abstraction of information in REST is a **resource**. Any information that can be named can be a **resource**: a document or image, a temporal service, a collection of other resources, a non-virtual object, and so on. Each **resource** is identified by a *resource identifier*. In practice, this will be a Uniform Resource Identifier [URI].
  - ii. **Manipulation of resources through representations:** Actions on **resources** are performed on **representations** of those **resources**. A **representation** is a sequence of bytes, plus *representation metadata* to describe those bytes. In practice, **representations** will be MIME media types [Media].
  - iii. **Self-descriptive messages:** All the information required to process a **request** is available in the **request**. This includes the host, message control metadata (like *Content-Length*), **representation** metadata and the **resource representation**.
  - iv. **Hypermedia as the engine of application state (HATEOAS):** The **client** knows only the starting URL of the **server**. All future interactions are discovered from **representations**. This allows the **server** to evolve separately from the **clients**.
4. **Layered system:** **Clients** and **servers** can be composed of hierarchical layers such that each component cannot see beyond the immediate layer with which it is interacting. It improves simplicity and scalability at the expense of efficiency.
  5. **Code-on-demand:** **Client** functionality can be extended by downloading and executing code in the form of applets or scripts. It improves simplicity and extensibility at the expense of visibility and security. This is an optional constraint.

The constraints of a RESTful architecture lead to simple, scalable, and evolvable systems. Simplicity means that few demands are placed on the cloud service consumer, whereas scalability and evolvability let the cloud service meet its rapid provisioning and releasing requirements, while incrementally expanding its services.

### 1.5.4 RESTful Authorization as a Service

Due to the pervasive nature of access control, Authorization-as-a-Service will result in many calls to the authorization **servers**. These **servers** must therefore perform and scale extremely well. Thus it makes sense to use a RESTful architecture for them.

This specification defines a profile for the use of XACML in a RESTful architecture, enabling the interoperability of RESTful Authorization-as-a-Service (AZaaS) solutions. The MIME media types [Media] available for representations of the various XACML constructs are defined separately [XACMLMedia].

## 1.6 Use Cases

This version of this profile will only consider the PEP and PDP. Later versions may involve other components of the XACML architecture, like the PAP and PIP.

### 1.6.1 PEP ↔ PDP

Line Of Business applications contain Policy Enforcement Points (PEPs) that interact with Policy Decision Points (PDPs) from various vendors. These PDPs may either be dedicated to the application, or be simultaneously offered to multiple applications (Authorization as a Service).



---

## 2 RESTful Services

{Normative}

### 2.1 Network Transport

The following URI SHALL be used as the identifier for the functionality specified in this section of this profile:

- urn:oasis:names:tc:xacml:3.0:profile:rest:http

Although not strictly required by REST, this specification mandates that HTTP MUST be used as the protocol to transport network messages [HTTP] between *client* and *server*.

For additional security, it is RECOMMENDED that SSL/TLS be used [HTTPS]. See section 3, Security Considerations, for more on securing the RESTful interactions.

Note that additional transport protocols are allowed but outside the scope of this profile.

### 2.2 Resources

The following sections describe the mandatory and optional *resources* that this profile defines. Each section defines which operations are supported on the *resource*, and what their requirements are. In particular, HTTP status codes [HTTP] define success or failure of the operation. See section 3, Security Considerations, for information on securing the RESTful interactions and representations.

#### 2.2.1 Entry Point

The following URI SHALL be used as the identifier for the functionality specified in this section of this Profile:

- urn:oasis:names:tc:xacml:3.0:profile:rest:home

| Operation | Request Body | Response Body     | Description | Status Codes                 |
|-----------|--------------|-------------------|-------------|------------------------------|
| GET       |              | XACML entry point |             | 200, 400, 401, 403, 406, 5xx |

To enable the discoverability requirement, a RESTful XACML system MUST have a single entry point at a known location [HomeDocument]. It is RECOMMENDED that the location of the entry point remain fixed, even as the service evolves, to allow older clients to remain functional. Each implementation of this profile MUST document the location of the entry point.

Note that the XACML entry point MAY be part of a larger RESTful system. In that case, the entry point location is not known in advance, but discovered from the enclosing system. The link relation <http://docs.oasis-open.org/ns/xacml/relation/home> SHALL be used for links to this resource. The documentation SHOULD contain information on how to discover the XACML entry point using this link relation.

The XACML entry point representation that is returned SHOULD NOT contain anything other than links to other *resources* specified in this profile.

#### 2.2.2 Policy Decision Point

The following URI SHALL be used as the identifier for the functionality specified in this section of this profile:

- urn:oasis:names:tc:xacml:3.0:profile:rest:pdp

The link relation type for links to this **resource** is  
<http://docs.oasis-open.org/ns/xacml/relation/pdp>.

| Operation | Request Body  | Response Body  | Description                      | Status Codes                      |
|-----------|---------------|----------------|----------------------------------|-----------------------------------|
| POST      | XACML request | XACML response | Makes an access control decision | 200, 400, 401, 403, 406, 415, 5xx |

A **server** MUST support `<Request>` from XACML core [**XACMLv3**] as the XACML request in the **request** body.

A **server** MAY additionally support `<XACMLAuthzDecisionQuery>` from the SAML Profile [**SAML4XACML**] as the XACML request. When `<XACMLAuthzDecisionQuery>` is used, requests and responses can be correlated using the request's ID and the response's `InResponseTo` attributes. When `<Request>` is used, this additional functionality is not available and the PEP must either use a new TCP/IP session, or wait with sending a request over the current session until the response for the previous request is received.

The processing and response MUST be as specified in the respective specification, either [**XACMLv3**] or [**SAML4XACML**].

Note that success of the HTTP operation (i.e. status code 200) doesn't mean that authorization is granted. It means that the **response** body is valid, and that the **response** body contains the XACML decision, which could be `Deny`. Likewise, a status code of 403 doesn't imply a XACML decision of `Deny`, but instead means that the user is not allowed to ask the PDP for an access decision.

Also note that, although this operation uses `POST`, it is both idempotent and safe [**HTTP**].

## 2.3 Representations

MIME media types defined for XACML in [**XACMLMedia**] or elsewhere MUST be used to represent **resources**. Whenever a **representation** is not available in that specification, a conforming implementation MAY chose its own representation. However, this specification will define constraints that such a **representation** MUST adhere to.

### 2.3.1 Linking

A fundamental concept in a RESTful architecture is that of linking between **resources** [**REST**].

For XML based **representations**, links MUST follow the Atom Syndication Format [**Atom**]. The link relation types [**WebLink**] for the services in this specification are given in their respective sections below. For instance, a link to the PDP could be

```
<atom:link rel="http://docs.oasis-open.org/ns/xacml/relation/pdp"
  href="/authorization/pdp"/>
```

For JSON based **representations**, links MUST map from Atom XML to JSON. For instance, a link to the PDP could be

```
{
  "link": {
    rel: "http://docs.oasis-open.org/ns/xacml/relation/pdp",
    href: "/authorization/pdp"
  }
}
```

Likewise, other **representations** SHOULD follow Atom as closely as possible.

Whenever it is not possible to add links to a **representation**, for instance because the **representation** must conform to a schema that doesn't support links, or because the **representation** is binary, links MUST be added using the `Link` HTTP header [**WebLink**]. In case of multiple links, the `title` attribute of the `Link` header field MAY be used to correlate the link to an item in the representation.

## 2.3.2 Entry Point

The **representation** of the entry point **resource** SHOULD NOT contain anything other than links to other **resources** specified by this profile.

## 2.4 Examples

### 2.4.1 Obtain an Access Decision

The following is a sequence of REST calls to obtain an authorization decision from a PDP. The **client** starts by accessing the entry point:

```
GET /authorization HTTP/1.0
Host: www.example.com
Accept: application/xml
Content-Length: 0
```

To which the **server** responds:

```
HTTP/1.0 200 OK
Content-Type: application/xml
Content-Length: <nnnn>

<resources xmlns="http://ietf.org/ns/home-documents"
  xmlns:atom="http://www.w3.org/2005/Atom">
  <resource rel="http://docs.oasis-open.org/ns/xacml/relation/pdp">
    <atom:link href="/authorization/pdp"/>
  </resource>
</resources>
```

The **client** looks for a resource with relation type `http://docs.oasis-open.org/ns/xacml/relation/pdp` and posts the XACML request to it:

```
POST /authorization/pdp HTTP/1.0
Host: www.example.com
Accept: application/xacml+xml; version=3.0
Content-Type: application/xacml+xml; version=3.0
Content-Length: <nnnn>

<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
  <!-- XACML request -->
</Request>
```

And finally the **server** responds with the access decision:

```
HTTP/1.0 200 OK
Content-Type: application/xacml+xml; version=3.0
Content-Length: <nnnn>

<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
  <!-- XACML response -->
</Response>
```

---

## 3 Security Considerations

{Non-normative}

Security and privacy considerations for the use of XACML in general are defined in [XACMLv3]. This section describes some additional considerations that have to do with the networked nature of a RESTful architecture, together with the administrative capabilities set out by this profile.

### 3.1 Network Transport

The use of SSL/TLS [HTTPS] is RECOMMENDED to protect data as it is transferred across the network.

### 3.2 Authentication

This specification leaves the issue open of how to authenticate. Implementations MUST document how they handle authentication.

HTTP status code 401 (Unauthorized) [HTTP] MAY be used to indicate that an operation on a **resource** is denied because the requestor is not authenticated. However, the problem of authentication over HTTP is not completely solved. [HTTPAuthN] defines Basic and Digest authentication. Basic authentication MUST NOT be used, since it sends the password in plain text over the network. Digest authentication MAY be used.

Additional standards like [OpenID], [SAMLv2] or [SASL] MAY be used instead of or in addition to HTTP Digest authentication.

### 3.3 Authorization

This specification RECOMMENDS that authorization be implemented using XACML. Implementations can perform authorization based upon the identity of the requestor, as well as on any appropriate additional, trusted, attribute. The use of the XACML Administration and Delegation Profile [Admin] is RECOMMENDED.

HTTP status code 403 (Forbidden) [HTTP] MUST be used to indicate that an operation on a **resource** is denied because the requestor is not authorized.

Authorization SHOULD be used to exclude from the **response** any links to **resources** that the requestor is not allowed to retrieve.

### 3.4 Non-Repudiation

In some situations it is important to have an audit trail of access decisions that were made. This audit trail must be at least tamper-evident. For this purpose, the SAML Profile for XACML [SAML4XACML] can be used to sign the access request and response.

## 4 Conformance

{Non-normative}

### 4.1 Conformance Clauses

This section lists those portions of the specification that **MUST** be included in an implementation of a **server** that claims to conform to this profile.

| Identifier                                     | M/O |
|--|-----|
| urn:oasis:names:tc:xacml:3.0:profile:rest:http | M   |
| urn:oasis:names:tc:xacml:3.0:profile:rest:home | M   |
| urn:oasis:names:tc:xacml:3.0:profile:rest:pdp  | M   |

### 4.2 Test Assertions

This section lists test assertions [**TAG**] that help verify conformance to this specification.

#### 4.2.1 Network Transport

|                           |  |
|---------------------------|--|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:http:client  |
| <b>Normative Source</b>   | The <b>client</b> must use HTTP when communicating with the <b>server</b> (From the more general source: HTTP MUST be used as the protocol to transport network messages between <b>client</b> and <b>server</b> ) |
| <b>Target</b>             | Network message from the <b>client</b>   |
| <b>Predicate</b>          | The [message] starts with an HTTP <b>request</b> line [ <b>HTTP</b> ]  |
| <b>Prescription Level</b> | mandatory  |

|                           |  |
|---------------------------|--|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:http:server  |
| <b>Normative Source</b>   | The <b>server</b> must use HTTP when communicating with the <b>client</b> (From the more general source: HTTP MUST be used as the protocol to transport network messages between <b>client</b> and <b>server</b> ) |
| <b>Target</b>             | Network message from the <b>server</b>   |
| <b>Predicate</b>          | The [message] starts with an HTTP <b>response</b> line [ <b>HTTP</b> ]   |
| <b>Prescription Level</b> | Mandatory  |

#### 4.2.2 Entry Point

|                         |  |
|-------------------------|--|
| <b>Id</b>               | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:home:documentation   |
| <b>Normative Source</b> | A RESTful XACML system <b>MUST</b> have a single entry point at a known location<br>Each implementation of this profile <b>MUST</b> document the location of the entry point |
| <b>Target</b>           | <b>server</b> documentation  |
| <b>Predicate</b>        | The [documentation] lists a (procedure for discovering a) single entry point URL at which the <b>server</b> can be accessed  |

|                           |           |
|---------------------------|-----------|
| <b>Prescription Level</b> | mandatory |
|---------------------------|-----------|

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:home:status |
| <b>Normative Source</b>   | GET on the home location MUST return status code 200            |
| <b>Target</b>             | <b>Response</b> to GET <b>request</b> on the home location      |
| <b>Predicate</b>          | The HTTP status code in the [response] is 200                   |
| <b>Prescription Level</b> | mandatory   |

|                           |  |
|---------------------------|--|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:home:body                          |
| <b>Normative Source</b>   | GET on the home location MUST return a home document                                   |
| <b>Target</b>             | <b>Response</b> to GET <b>request</b> on the home location                             |
| <b>Predicate</b>          | The HTTP body in the [response] follows the home document schema <b>[HomeDocument]</b> |
| <b>Prescription Level</b> | mandatory  |

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:home:pdp  |
| <b>Normative Source</b>   | The XACML entry point representation SHOULD contain a link to the PDP   |
| <b>Target</b>             | <b>Response</b> to GET <b>request</b> on the home location  |
| <b>Predicate</b>          | The home document in the [response] body contains a resource with link relation <a href="http://docs.oasis-open.org/ns/xacml/relation/pdp">http://docs.oasis-open.org/ns/xacml/relation/pdp</a> and a valid URL |
| <b>Prescription Level</b> | mandatory   |

### 4.2.3 Policy Decision Point

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:pdp:xacml:status                            |
| <b>Normative Source</b>   | POST on the PDP with a valid XACML request MUST return status code 200                          |
| <b>Target</b>             | <b>Response</b> to POST <b>request</b> on the PDP location with valid XACML request in the body |
| <b>Predicate</b>          | The HTTP status code in the [response] is 200   |
| <b>Prescription Level</b> | mandatory   |

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:pdp:xacml:body                              |
| <b>Normative Source</b>   | POST on the PDP with a valid XACML request MUST return a valid XACML response in the body       |
| <b>Target</b>             | <b>Response</b> to POST <b>request</b> on the PDP location with valid XACML request in the body |
| <b>Predicate</b>          | The HTTP body in the [response] is a valid XACML response                                       |
| <b>Prescription Level</b> | mandatory   |

|                         |   |
|-------------------------|---|
| <b>Id</b>               | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:pdp:xacml:invalid                   |
| <b>Normative Source</b> | POST on the PDP with an invalid XACML request MUST return status code 400 (Bad Request) |

|                           |   |
|---------------------------|---|
| <b>Target</b>             | <b>Response</b> to <code>POST request</code> on the PDP location with invalid XACML request in the body |
| <b>Predicate</b>          | The HTTP status code in the [response] is 400   |
| <b>Prescription Level</b> | mandatory   |

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:pdp:saml:status   |
| <b>Normative Source</b>   | <code>POST</code> on the PDP with a valid XACML request <b>MUST</b> return status code 200  |
| <b>Target</b>             | <b>Response</b> to <code>POST request</code> on the PDP location with valid XACML request wrapped in a <code>xacml-samlp:XACMLAuthzDecisionQuery</code> in the body |
| <b>Predicate</b>          | The HTTP status code in the [response] is 200   |
| <b>Prescription Level</b> | optional  |

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:pdp:saml:body   |
| <b>Normative Source</b>   | <code>POST</code> on the PDP with a valid XACML request <b>MUST</b> return a valid XACML response in the body   |
| <b>Target</b>             | <b>Response</b> to <code>POST request</code> on the PDP location with valid XACML request wrapped in a <code>xacml-samlp:XACMLAuthzDecisionQuery</code> in the body |
| <b>Predicate</b>          | The HTTP body in the [response] is a valid XACML response wrapped in a <code>samlp:Response</code>  |
| <b>Prescription Level</b> | optional  |

|                           |   |
|---------------------------|---|
| <b>Id</b>                 | urn:oasis:names:tc:xacml:3.0:profile:rest:assertion:pdp:saml:invalid  |
| <b>Normative Source</b>   | <code>POST</code> on the PDP with an invalid XACML request <b>MUST</b> return status code 400 (Bad Request)   |
| <b>Target</b>             | <b>Response</b> to <code>POST request</code> on the PDP location with invalid XACML request wrapped in a <code>xacml-samlp:XACMLAuthzDecisionQuery</code> in the body |
| <b>Predicate</b>          | The HTTP status code in the [response] is 400   |
| <b>Prescription Level</b> | optional  |

---

## Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

**Participants:**

David Brossard, Axiomatics  
Jean-Paul Buu-Sao, TSCP  
Jacques Durand, Fujitsu  
Craig Forster, IBM  
Hal Lockhart, Oracle  
Danny Thorpe, Dell  
Erik Wilde, EMC



---

## Appendix B. Revision History

| Revision | Date       | Editor        | Changes Made  |
|----------|------------|---------------|---|
| WD01     | 2012-02-14 | Rémon Sinnema | Defined use cases   |
| WD02     | 2012-04-24 | Rémon Sinnema | Initial full draft  |
| WD03     | 2012-05-03 | Rémon Sinnema | Fixed typos<br>Renamed Use Cases section to Rationale<br>Introduced Use Cases section<br>Moved everything representation related out of the section on resources<br>Added examples<br>Improved authorization section  |
| WD04     | 2012-05-22 | Rémon Sinnema | Conformance section should succinctly indicate what needs to be implemented<br>Added platform use case<br>Added policy version resource   |
| WD05     | 2012-05-31 | Rémon Sinnema | PDP is now optional, allowing PAP-only servers<br>Added explanatory text for delete example<br>Added note on policies contained within policy sets<br>Added note that supplied policies must be valid according to the policy schema<br>Improved wording in Security section<br>Added "lost" paragraph from WD02 about the contents of the entry point resource<br>Added text on different types of PAPs<br>Added text on policy (version) equality<br>Added use of HTTP to conformance section |
| WD06     | 2012-10-9  | Rémon Sinnema | Added domain terms<br>Added section on test assertions<br>Removed policy administration related text<br>Updated text to better fit the home document standard<br>Added section on non-repudiation<br>Replaced reference to XACML Media Types Profile with URL of Internet Draft<br>Added text on embedding XACML REST in a larger RESTful system  |