XACML profile for an htaccess authorization source

2 juli 2013

Author:
O. Koeroo

version: 2.0

Description

This profile describes the attributes passed to and from an XACML service which is uses an htaccess file as authorization source. The origin of this profile is the Access rights Management System (AMS) of The Language Archive at the Max Planck Institute (MPI) from Nijmegen.

Attributes

There are attribute identifiers and values to be send to and from an XACML which are respectively input to an XACML service and output of an XACML service. This profile is agnostic to the XACMLv2, XACMLv3 with or without the XACML-REST profile and/or XACML-JSON profile.

Recommended parental profiles

To keep XACML as lightweight as possible both on the wire and as software stack the following recommendation are given to steer the software stack and parenting profile selection. The recommendation are ordered from most significant to least significant to achieve a simple to implement software stack:

1. XACML-REST: a REST based XACML on-the-wire profile which eliminates the SOAP-Envelope and SAML2 binding. The XACMLv2 and XACMLv3 should normally be bound to the SAML2 attributes. Both the SOAP and SAML layers add overhead on the wire and add software stack complexity without benefits.
2. XACMLv3: The third major version of XACML uses different attribute identifiers and also as a concept of responding with an “Advice” where XACMLv2 only features “Obligations”. Also the third XACML version matches the profile bindings with XACML-JSON and XACML-REST.
3. XACML-JSON: A profile that exchanges the XML-based request and response messages for JSON. The use of JSON makes the request and response message slimmer by using the strict formatting rules of JSON. Because of its simplicity it aids non-XACML specific clients to work with XACML without the need for formal parser.

AMS profile

Request

The request message from the PEP (XACML client) to the XACML service for the AMS system will need to following mandatory attributes to operate.

x-urn:nl:mpi:tla:xacml:subject:username

The username identifying the end-user on this system. For example an edupersonprincipalname. The attribute is scoped to the Subject category of the Request message.

x-urn:nl:mpi:tla:xacml:action:access

Indicates the requested access type of the file to be access. The attribute is scoped to the Action category of the Request message. The options are distinct access for reading, writing and read+writing of files. The values are explicitly profiled to the following values:

1. **x-urn:nl:mpi:tla:xacml:action:access:read**
   Request read-only access to the resource.
2. **x-urn:nl:mpi:tla:xacml:action:access:write**
   Request write-only access to the resource.
3. **x-urn:nl:mpi:tla:xacml:action:access:readwrite**
   Request read and write access to the resource.

Note: Supporting write-only is optional.

x-urn:nl:mpi:tla:xacml:resource:directory

The directory in which the local file (x-urn:nl:mpi:tla:xacml:resource:file) resides. The attribute is scoped to the Resource category of the Request message.

x-urn:nl:mpi:tla:xacml:resource:file

The name of a logical file located in a directory indicted by x-urn:nl:mpi:tla:xacml:resource:directory. The attribute is scoped to the Resource category of the Request message.

Response

The response message of the XACML service will indicate a Permit, Indeterminate or Deny decision.

Permit

On return of a Permit decision the username is allowed to perform the httpmethod on the directory and file resource.

Deny

On return of a Deny decision this is not allowed.

InApplicable

On return of a InApplicable decision the PEP is expected to treat this as a Deny. The difference is that InApplicable means to have no policy statement available for the queried resource.

Indeterminate

On return of an Indeterminate decision the PEP is expected to treat this as a Deny. The

difference is that Indeterminate means to indicate a problem in the policy evaluation itself.