GWD-C
FEDSEC-CG
fedsec-cg@ogf.org

Brian Bockelman, University of Lincoln-Nebraska
Dave Dykstra, Fermilab
Gabriele Garzoglio, Fermilab
David Groep, Nikhef
Mischa Sallé, Nikhef
??? 2015

Extension to the XACML AuthZ Interoperability Profile

Status of This Document

Group Working Draft (GWD)

Copyright Notice

Abstract

This document describes additions and clarifications to the XACML Grid Authorization Interoperability profile[3]. It is not intended as a replacement of the old profile, but as an addition to it. The main additions are a new obligation *account*, to provide account information based on names instead of numerical IDs, and a specification how the client can pass information on the level of trust of subject attributes. Furthermore this document clarifies a few ambiguities in the original specification.

Contents

1 Introduction

The XACML Authorization Interoperability profile[3] was developed a number of years ago in a collaborative effort of OSG, EGEE and Globus, in order to agree on a common set of obligations and attributes to be used in the Grid authorisation infrastructure. It is currently used both by OSG and partly by EGI (as successor of EGEE) and has resulted among other things in the use of the same client software on both sites of the Atlantic.

Now that it has been successfully used for a number of years, a few shortcomings have come to light, which warrant extensions and adaptations. These changes will be described in the different subsections of Section 4. In Section 5 we will give their respective motivations.

A further motivation for adapting the profile could come from the Argus framework, the authorisation framework used by the majority of the European sites. Due to similar considerations as those expressed here, in particular the lack of certain obligations, the Argus collaboration has introduced a different profile[4]. By extending the interoperability profile to cover such obligations, we open the way to at some point unify the two profiles.

2 Notational conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [1], except that the words do not appear in uppercase.

The namespace of the profile is unchanged:

- Obligations have full ID
  http://authz-interop.org/xacml/obligation/≪ObligationID≫
- Attributes have full ID
  http://authz-interop.org/xacml/attribute/≪AttributeID≫

We will mostly use only the shortened IDs in this document.

3 Security considerations

The security considerations as described in the existing profile [3], remain fully valid.

Additionally, the extension described in Section 4.6 provides (among others) means to inform the server about the reliability, or lack of that, of the information passed from the client to the server. Hence the server can response adequately even to unverified requests by optionally

doing this verification itself. Also, in cases it is not able to do so, it can fail, preventing unauthorised access.

Furthermore, the clarifications described in the different subsections of Section 4 prevent misconfigurations which could result in granting users the wrong access rights. By properly defining the behaviour in complicated situations, this can be prevented.

4 Extensions and adaptations

This section describes the different changes with respect to the previous interoperability profile. The rationale for the different changes is described in corresponding subsections of Section 5.

4.1 Full specification of *username* obligation

The specification of the obligation *username* (paragraph 7.5, reference [3]) only describes that it should set the username as given by the attribute *username*. The profile should be amended to read that the client sets the full account, according to `getpwent()` information [5] for the given username, i.e. UID, pGID and optionally sGIDs.

4.2 New *account* obligation

An obligation is required that can explicitly set primary or secondary groupnames, i.e. based on groupname instead of GID. To provide this, the profile should be extended with a new obligation *account* with attributes *username*, *primary-groupname* and *secondary-groupnames*. Each attribute is optional. The server may send the obligation without any attributes, in which case the client must verify that it has support for the obligation and fail if it has not. See also Section 4.5

ID: *account*

Full Obligation ID: *http://authz-interop.org/xacml/obligation/account*

Attributes:

> **ID** : *username*
>
> **Description:** username of the resulting account.
>
> **Full Attribute ID:** *http://authz-interop.org/xacml/attribute/username*
>
> **Type:** string
>
> **Multiplicity:** 0 . . . 1

ID : *primary-groupname*

Description: primary groupname of the resulting account.

Full Attribute ID: *http://authz-interop.org/xacml/attribute/primary-groupname*

Type: string

Multiplicity: 0 . . . 1

ID : *secondary-groupname*

Description: secondary groupname of the resulting account.

Full Attribute ID: *http://authz-interop.org/xacml/attribute/secondary-groupname*

Type: string

Multiplicity: 0 . . . N

4.3 Behaviour multiple primary group (and username) attributes

The profile should be extended to enforce the same behaviour for primary GIDs as it prescribes for multiple UIDs (paragraphs 7.3 and 7.5, reference [3]):

1. Each obligation can contain at most one pGID setting attribute
2. If multiple obligations set a primary GID, either directly or indirectly, all resulting pGIDs should be identical.

4.4 Dependencies of the *secondary-gids* obligation

The old specification of the *secondary-gids* obligation stated this obligation needs the *uidgid* obligation. This requirement is removed: the server may send back a response containing an incomplete mapping (or no mapping at all). It is up to the client to determine whether this is a failure or not, and the client may obtain the actual mapping via other means.

Additionally, the server may also send back a combination of the *secondary-gids* together with another obligation than the *uidgid* obligation to produce a complete mapping.

4.5 Obligation attributes and their multiplicities

The multiplicity of the attributes for the different obligations shall be the following:

ObligationID: *username*[1]

AttributeID: *username*

Multiplicity: 0 . . . 1

ObligationID: *uidgid*[2]

AttributeID: *posix-uid*

Multiplicity: 0 . . . 1

AttributeID: *posix-gid*

Multiplicity: 0 . . . 1

ObligationID: *secondary-gids*[3]

AttributeID: *posix-gid*

Multiplicity: 0 . . . N

ObligationID: *account*

AttributeID: *username*

Multiplicity: 0 . . . 1

AttributeID: *primary-groupname*

Multiplicity: 0 . . . 1

AttributeID: *secondary-groupname*

Multiplicity: 0 . . . N

Each obligation may be send by the server without any attributes, in which case the client must verify that it has support for that obligation and fail if it has not.

4.6 Verification of subject attributes on client side

By optionally setting an issuer element in a subject attribute in the request (see paragraph 6.7 in reference [2]), the client can inform the server about the reliability of the corresponding attribute. We distinguish the following cases:

[1] §7.5, ref. [3]
[2] §7.3, ref. [3]
[3] §7.4, ref. [3]

1. the client has no knowledge about the reliability of the attribute, i.e. it may or it may not be verified. In this case the client must not specify an issuer element.
2. the client can reliably state that the attribute is *not* verified. In this case the client should provide the issuer element with the special value *http://authz-interop.org/xacml/issuer/none*.
3. the client can reliably state that the attribute *is* verified. In this case the client should provide the issuer element with a value depending on the type of attribute:
   (a) for appropriate non-VOMS attributes extracted from the proxy certificate, the value must be set to the issuer-DN of the EEC of the proxy chain, i.e. to the *subject-x509-issuer* subject attribute, see paragraph 6.1.4 in reference [3].
   (b) for appropriate VOMS attributes extracted from the VOMS AC inside the proxy certificate, the value must be set to the DN of the VOMS service that signed the corresponding AC, i.e. to the *voms-signing-subject* subject attribute, see paragraph 6.1.6 in reference [3].

The full list of subject attributes with their respective issuers is given in the following table:

Attribute	**Issuer element**
subject-x509-id	*subject-x509-issuer*
subject-x509-issuer	issuer-DN of CA certificate
validity-not-before	*subject-x509-issuer*
validity-not-after	*subject-x509-issuer*
certificate-serial-number	*subject-x509-issuer*
ca-serial-number	issuer-DN of CA certificate
ca-policy-oid	*subject-x509-issuer*
cert-chain	*subject-x509-issuer*
vo	*voms-signing-subject*
voms-signing-subject	*voms-signing-issuer*
voms-signing-issuer	issuer-DN of VOMS signing CA
voms-fqan	*voms-signing-subject*
voms-primary-fqan	*voms-signing-subject*
voms-dns-port	*voms-signing-subject*
subject-condor-canonical-name-id	FQDN or host certificate subject-DN of the service

4.7 Requirement on attributes for backwards compatibility

The interoperability profile explicitly gives a list of best practise recommendations in paragraph 4.2. Although implied it does not mention explicitly what behaviour is expected from a client if it receives a known obligation with unknown attributes. The behaviour should be that the client fails. Hence it must be strongly discouraged to add extra attributes to existing obligations. Instead, when existing obligations cannot fulfil a use case, new obligations must be created.

4.8 Pilot job environment context attributes

The list of pilot-job environment context attributes given in Appendix B, section 9.6 of the interoperability profile, is missing a number of pilot-job attributes corresponding to their subject context attribute counterparts. The list to be added is

http://authz-interop.org/xacml/environment/pilot-job/certificate-serial-number
http://authz-interop.org/xacml/environment/pilot-job/validity-not-before
http://authz-interop.org/xacml/environment/pilot-job/validity-not-after

The latter

http://authz-interop.org/xacml/environment/pilot-job/ca-serial-number
http://authz-interop.org/xacml/environment/pilot-job/voms-dns-port
http://authz-interop.org/xacml/environment/pilot-job/ca-policy-oid
http://authz-interop.org/xacml/environment/pilot-job/cert-chain

4 correspond to the optional subject attributes from section 6.2 in the profile.

Furthermore, as an alternative to the requirement for such environment attributes for pilot jobs, as stated in section 6.5.3 in the profile, the pilot job invoker identity information may also be obtained from the client-side certificate, in case the connection between client and server is using mutually authenticated certificate-based authentication. If the client uses a host certificate as its certificate, this identity may be obtained in the form of a hostname, as long as the pilot job invoker identity is reliable recorded on the client host. At least one of the two alternatives, i.e. environment attributes or client certificate, must be used.

5 Rationale

This section describes the rationale for the different changes described in Section 4. The different subsections in this section correspond to the changes described there.

5.1 Rationale: Full specification of *username* obligation

Both LCMAPS plugins (lcmaps-plugins-scas-client and lcmaps-plugins-c-pep) use an implementation that sets a complete account belonging to the username, according to `getpwent()` information [5]. Changing this behaviour would change the effect of the obligation in a backwards incompatible way. Note that the profile only supports passing supported obligationIDs to the server, not the corresponding attributeIDs, while clients typically fail on unrecognised attributes.

The new behaviour is also in line with 'classic' Globus behaviour, the Globus callout mechanism typically returns a single username, which is used to determine the complete account.

5.2 Rationale: New *account* obligation

The rationale for introducing a new obligation is motivated by the requirement to keep the username obligation implementation backwards compatible, see Subsection 5.1. Hence we cannot add additional primary and secondary groupname attributes to the username obligation.

Alternatively, introducing separate new obligations for the primary and secondary groupnames, analogously to the GID obligations, would have let to an asymmetry with respect to the username obligation: the username obligation would set the whole account, the groupname obligations only one or more groups.

The choice for a single new obligation with optional attributes leads to the greatest flexibility and the least amount of needed client code, since it can be handled with a single new obligation handler. Furthermore, it is very similar to the *http://glite.org/xacml/obligation/local-environment-map/posix* obligation in the Argus worker node profile (paragraph 3.5.1, ref. [4]).

5.3 Rationale: Behaviour multiple primary group attributes

The profile only described the behaviour in case multiple obligations set a UID, in which case either all of them must be identical, or the client should fail. The profile did not mention similar behaviour in case of multiple pGIDs, since it only contained a single obligation being capable of that, the uidgid obligation (even though in practise also the username obligation sets one). Since obligations are unordered in the XACML2 standard, there is a need to determine the behaviour. The new behaviour is the same as that for the UID.

5.4 Rationale: Dependencies of the *secondary-gids* obligation

For greater flexibility, any combination of credential mapping obligations is allowed as long as they are not conflicting.

5.5 Rationale: Obligation attributes and their multiplicities

It was unclear whether obligations were allowed to have no attributes, except for the *secondary-gids*, for which it was stated explicitly that the list of GIDs may be empty. Hence we formalise the full set of multiplicities. Changing the multiplicity for the attribute of the *secondary-gids* obligation would break current SCAS implementations, hence we keep the existing behaviour.

5.6 Rationale: Verification of subject attributes on client side

In the OSG scenario, the VOMS credentials are passed from the client to the server unverified. The user effectively passes a list of requested FQANs to the server (GUMS), and it is the task of the server to verify whether the user is allowed them.

In the European scenario, the client (gLExec) verifies the proxy, including its VOMS part. Hence the entire proxy chain is fully verified on client side, and the server (SCAS) can rely on the validity of the received credentials.

It is useful to have the ability to pass to the server who is responsible for the verification. This could speed-up GUMS performance (it does not need to verify them again if they are already verified) and provide feedback to the SCAS in case of a misconfiguration that would lead to reliance on unverified credentials.

A further motivation for adding issuer elements to the attributes comes from proxies containing multiple VOMS ACs. In those cases, having the issuer is the only way of telling which attributes belong to which VO.

5.7 Rationale: Pilot job environment context attributes

The list of *environment/pilot-job/** attributes was incomplete making it impossible to put e.g. the pilot-job certificate chain into the environment.

In most deployment scenarios, the client is talking to the server over an encrypted, mutually authenticated connection, using client and server certificates. In the European scenario, the client certificate is typically a proxy belonging to the pilot-job user, and the server can obtain all the identity information from there. In the OSG scenario, the client certificate is typically a host certificate, but the pilot identity will then reliably be logged by e.g. gLExec on the client host.

5.7.1 Format and name-space

Although using RFC2253 [6] formatted x500name notation for DNs in the issuer elements would seem a more logical choice, this would constitute an incompatible change from the existing profile. Furthermore, obtaining RFC2253 formatted DNs from the current VOMS implementation is rather involved and would require changes in multiple libraries.

Concerning the name-space of the special none issuer, we have a preference to stay with the same name-space as the rest of the profile, i.e. *http://authz-interop.org/xacml*.

5.8 Rationale: Requirement on attributes for backwards compatibility

Since the profile provides all the necessary means to stay backwards compatible and still exchange sufficient information about understood obligations, via the *pep-oblig-supported* environment attribute (paragraph 6.5.2, ref. [3]), we do not need to provide a separate environment attribute providing the profile version, such as is used by the Argus worker node profile (paragraph 3.1.1, ref. [4]). The use of the supported obligations attribute is more flexible: it provides fully namespaced obligation IDs, allowing even for mixing different profiles.

6 Glossary

UID:	User Identity
GID:	Group Identity
pGID:	Primary Group Identity
sGID:	Secondary Group Identity
EEC:	End Entity Certificate
DN:	Distinguished Name
VOMS:	Virtual Organisation Membership Service
AC:	Attribute Certificate
FQAN:	Fully Qualified Attribute Name
EGEE:	Enabling Grids for E-Science in Europe
EGI	European Grid Infrastructure
OSG:	Open Science Grid
GUMS:	Grid User Management System
SCAS:	Site Central Authorization Service
XACML:	eXtensible Access Control Markup Language
FQDN:	Fully Qualified Domain Name

7 Contributors

Brian Bockelman
University of Lincoln-Nebraska
1400 R Street
Lincoln, NE 68588
United States of America
Email: bbockelm@cse.unl.edu

Dave Dykstra
Fermilab
P.O.Box 500
Batavia, IL 60510-5011
United States of America
Email: dwd@fnal.gov

Gabriele Garzoglio

Fermilab
P.O.Box 500
Batavia, IL 60510-5011
United States of America
Email: garzogli@fnal.gov

David Groep
Nikhef
Postbus 41882
1009 DB Amsterdam
The Netherlands
Email: davidg@nikhef.nl

Mischa Sallé
Nikhef
Postbus 41882
1009 DB Amsterdam
The Netherlands
Email: msalle@nikhef.nl

8 Acknowledgements

This work is part of the research program of the Foundation for Fundamental Research on Matter (FOM) which is financially supported by the Netherlands Organisation for Scientific Research (NWO).

This work is part of the activities of the Dutch e-Infrastructure, which is financially supported by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Netherlands Organisation for Scientific Research, NWO) and the Dutch higher education and research partnership for network services and information and communication technology (SURF).

This work was partially supported by NSF grant #1148698.

Fermilab is operated by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the United States Department of Energy.

9 Intellectual Property Statement

The OGF 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. 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 specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

10 Disclaimer

This document and the information contained herein is provided on an "As Is" basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

11 Full Copyright Notice

12 References

[1] Scott Bradner. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119 (Best Current Practice), March 1997. URL `http://tools.ietf.org/html/rfc2119`.

[2] Tim Moses (editor). eXtensible Access Control Markup Language (XACML) Version 2.0, 2005. URL http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[3] R. Ananthakrishnan et al. An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids. GFD-CP.205, 2011. URL https://www.ogf.org/documents/GFD.205.pdf. http://cd-docdb.fnal.gov/cgi-bin/ShowDocument?docid=2952.

[4] Chad La Joie and Valery Tschopp. XACML Grid Worker NodeProfile, Version 1.0, 2010. URL https://edms.cern.ch/document/1058175.

[5] The IEEE and The Open Group. The Open Group Base Specifications Issue 7, IEEE Std 1003.1, 2013 Edition, endpwent, getpwent, setpwent - user database functions, 2013. URL http://pubs.opengroup.org/onlinepubs/9699919799/functions/endpwent.html.

[6] M. Wahl, S. Kille, and T. Howes. Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names. RFC 2253 (Proposed Standard), December 1997. URL http://tools.ietf.org/html/rfc2253.