GWD-C
Federated Security
fedsec-cg@ogf.org

Rachana Ananthakrishnan, Argonne National Laboratory
Gabriele Garzoglio *, Fermilab
Oscar Koeroo *, Nikhef
January 21, 2013
Protocol version 1.2

An XACML Attribute and Obligation Profile for Authorization Interoperability in Grids

Status

Group Final Draft (GFD).

Abstract

The goal of the Authorization Interoperability activity is providing interoperability between middleware and authorization infrastructures. This is achieved by designing and implementing an authorization protocol common to OSG VO services, EGEE, Globus, and Condor. This protocol is based on the SAML profile of XACML v2.0 [XACML]. The C library that implements the profile is provided by the Globus Toolkit security group; the JAVA library by the SWITCH group of the EGEE project. The EGEE project has evolved into the Distributed Computing Infrastructure (DCI) called EGI and the Technology Providers (TP) EMI and IGE.

The authorization protocol is used by Policy Enforcement Points (PEP), i.e. resource gateways, to interact with Policy Decision Points (PDP), i.e. repository of authorization policies. For each access request, the PDP informs the PEP on whether access is granted or denied and the conditions to be enforced if access if granted. These conditions are expressed in the form of XACML Obligations and are the mechanism to restrict privileges at Grid resources.

* Corresponding authors

1. Introduction

This document provides the specifications of Subject, Action, Resource, Environment, and Obligation attributes common to our groups. The attributes that we describe are commonly found and used in Grid scenarios; however, some of the attributes are implementation-specific and may be of significance only to a specific group, project, or software.

The authors acknowledge that some of the choices are not applicable to all authorization use cases. We do not exclude the possibility to update and extend these use cases, but, at this time, our focus is towards our production Grid infrastructures. The document focuses on X.509, VOMS, and POSIX-related credentials. For these reasons, this should be considered as an “experience” or “best practice” document to inform the community on the characteristics of an authorization profile that has worked in production since 2008. Considerations on how to upgrade this document are discussed in the “Upgradeability” section.
The profile described in this document has been implemented in GUMS [GUMS], SCAS [SCAS], SAZ [SAZ] and their client tools/middleware. These implementations and this profile have been used as a reference for developing the profiles used in Argus.

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 [BRADNER], except that the words do not appear in uppercase.

3. Security considerations

The protocol is intended to be used as a standardized means of requesting an authorization decision from a resource to an authorization service. The XACML version 2 document describes these roles as a Policy Enforcement Point (PEP) and Policy Decision Point (PDP).

The expected response from the PDP is a binary decision to “Permit” or “Deny” access to the requested resource. An XACML response with value “Indeterminate” or “Not Applicable” MUST be treated as a “Deny”. In the case where the requestor is allowed access to the resource the PDP MAY return XACML Obligations. All returned Obligations MUST be fulfilled by the resource that had sent the request. In the case where intermediate services are placed between the resource and authorization service then they MAY fulfill parts of the response.

A decision returned from an authorization service to a resource could result in a persistent allocation, for example the allocation of one account from a pre-configured limited account pool. An attack could use this effect to its advantage in the form of a denial of service attack. The impact of a denial of service attack is greatly dependent on the type of resources which was depleted.

To avoid easy replay attacks and message insertion and/or modification, the communication between the resource and authorization service MUST take place over an SSL-encrypted transport protocol. To ensure that the right resource and/or user is sending a request, the SSL-encrypted transport protocol MUST comply with RFC2818 (HTTP-over-TLS) and the client MUST authenticate the authorization service. The service MUST authenticate the client by presenting its End-Entity-Certificate or an RFC3820 (Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile) proxy certificate. The service MAY authorize the requestor by the credentials it presented during the SSL/TLS-handshake. An unsuccessful SSL-handshake MUST be handled as if the XACML layer resulted in a DENIED statement.

4. Upgradeability

This document describes a profile for authorization assertions targeting multiple resource types, such as computing elements, storage elements, and worker nodes. Such resources are controlled by resource gateway software, or policy enforcement points (PEP e.g. Globus gatekeeper, SRM, etc.). According to the XACML model, the PEPs are responsible for contacting a policy decision point (PDP) at the site and enforcing its authorization decisions.

In this section we discuss how we recommend addressing the problems of resource gateway upgrades and of profile upgrades.

4.1. Resource Gateways Upgrades

With the variety of PEPs discussed above and considering that the typical size of modern deployments consists of several hundreds nodes within a single administrative boundary, it is unavoidable that resource gateway software at a site will be upgraded at different times. This presents the following problem.

We foresee that the upgraded gateways will be able to enforce different / finer-grain authorization constraints, or “obligations”, from the site PDP, while the older gateways won’t be able to even understand such constraints. The XACML model, however, requires that a PEP must reject the authorization request, if it does not understand one of the obligations from the PDP. How can we allow a PDP to return the finer-grain obligations to the upgraded PEPs, which understand them, and to return old obligations to the old PEPs?

In this profile we provide the following solution. PEPs can communicate to the PDP the list of obligations that they understand, via the attribute SupportedObligations from the XACML environment request context. Such list can be considered by the PDP as advisory on the PEP capabilities, thus allowing the distinction between old and upgraded resource gateway software. If new PEP software is backward compatible, this mechanism allows resources and PDPs to be upgraded at different times. More details of this attribute are discussed in the Environment section.

4.2. Profile Upgrades

We envision that this profile will evolve with time: new resources, actions, and subject attributes will be inevitably added to address new needs for access authorization. In order for the implementations of this profile to maintain their properties of interoperability within our group, we recommend the following practices:

- Attributes and obligations can be added to this profile, upon discussion within the group
- Attributes and obligation should not be removed from this profile, unless expressly agreed by the group. Removing attributes and obligations has potentially more disruptive consequences than adding new ones
- PDPs that implement the old profile, will ignore new attributes
- PDPs that implement the new profile should not require new attributes in order to return old obligations. The SupportedObligations attribute from the PEP can guide the choice of a compatible set of obligations to return.
- PEPs that implement the old profile should not be affected if the PDP is backward compatible and uses the SupportedObligations attribute from the PEP.

- PEPs that implement the new profile are recommended to maintain handlers for old obligations, in order to avoid authorization rejections due to unknown (old) obligations. Each PEP implementer will have to decide how backward compatible the PEP should be.

5. Namespace

The following sections discuss the Attribute Namespace for this profile.

5.1. Attribute Namespace

This section describes the prefixes used for both URL and URN namespace styles for the authorization interoperability activities. All the attributes introduced by this profile are in URL notation. The profile still uses URN notation for those attributes considered standard, such as urn:oasis:names:tc:xacml:1.0:resource:resource-id .

Each attribute described in this document has an associated attribute name (attribute-id or obligation-id). This name needs to be concatenated with the following prefix when implementing this profile.
URL root prefix: "http://authz-interop.org/xacml"

This namespace prefix is meant to be generic and not limited to the Grid-related use cases described in this document. People interested in using this namespace for use cases external to this document should contact David Groep[1], owner of the "authz-interop.org" namespace.

5.2. URI choice: URN vs. URL

In the previous section, we define a namespace for the authorization interoperability activities in URL notation. Nevertheless, we acknowledge that both URL and URN notations present advantages and disadvantages.

A URN style namespace is preferred for reasons of compatibility with standards bodies like OASIS and IETF; however, using a URN requires the formal registration of the namespace with bodies like IANA. This approach has been considered for the medium to long term for web-wide standardization of the Grid use cases described in this document. After 5 years using this profile in production environments, though, the need for introducing URN notation never materialized and was dropped from the profile.

A URL style namespace is preferred because it does not require the registration of a namespace with any standardization body. The uniqueness of the namespace is derived by the uniqueness of the domain name. Moreover, additional services for XML schema resolution and location can be established at the registered domain. For example, both OGF and W3C support direct mapping and resolution of registered XML infoset schemas into URLs. Infoset namespace is described in GFD.84, which also specifies the schema repository and service location as http://schemas.ogf.org/.

[1] David Groep, Nikhef, Science Park 105, 1098XG, Amsterdam. Email: davidg@nikhef.nl

6. XACML Request

The following sections define the authorization interoperability attributes for the XACML request message. It defines attributes for the subject, action, resource, and environment contexts.
In general, unless otherwise noted, the attributes in the request and response are expected to hold only one value (e.g. “subject-x509-id”). Should the message hold more than one value, the system will only use the first of the list, ignoring all subsequent ones. The profile assumes that all the attributes send in a request message are verified and authenticated by the client tools before being used in the authorization request.

6.1. Subject

A PEP uses the subject contexts to declare for what entity the authorization decision is requested. The subject section in the request message contains multiple attributes. Each attribute is given a name or identifier, a datatype, and a value. The types are chosen from the available datatypes in the XML Schema [XMLSchema].
The subject attributes are used to determine an authorization decision, but not all attributes in the subject section need to play a role in the decision. All attributes MUST be present in the request, if the information is available when composing the request; PDPs consider attributes that are not present in the request as having a null value.
If subject-condor-canonical-name-id is present, the other attributes do not need to be present.
Note: in some of the attributes, we chose to add the prefix “subject-“ to the name (e.g. subject-x509-id) to underline the context of the attribute in the name itself. Despite the fact that this is redundant since these attributes are in the <subject> context, we found that this clarified our verbal communication.

6.1.1. Namespace Prefix Expansion

By concatenation with the URL root-prefixes, the namespace prefix of subject attributes is expanded to the following prefix:

URL based namespace prefix: <URL root prefix> + "/subject"

The namespace of each of the following attribute-ids is derived by concatenating this prefix with the given attribute-id name.

6.1.2. Subject-x509-id

This attribute holds the Distinguished Name (DN) of the user. This DN is the subject extracted from the user’s certificate. This attribute is implicitly linked in this profile with subject-x509-issuer attribute. The datatype of this attribute is string to accommodate the OpenSSL oneline representation of slash-separated Relative Distinguished Names.
We acknowledge that the most commonly used representation for this attribute is the X.500 datatype; however, we decide not to use it because the slash-separated representation is the defacto standard in our environment. Tools and services are free to support the subject-x509-id as X.500 datatype besides the OpenSSL online representation. In that case the Datatype MUST be set to X509Name.

ID: subject-x509-id
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/subject-x509-id
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/subject-x509-id"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>/O=dutchgrid/O=users/O=nikhef/CN=Oscar Koeroo</AttributeValue>
</Attribute>
```

6.1.3. Subject-condor-canonical-name-id

This attribute is specific for the authorization call-out implementation of the HTCondor [HTCondor] system. This attributes holds the identity of a user in the HTCondor system and will be handled by the authorization call-out system as an opaque identifier i.e. it will be interpreted only by the HTCondor system. The representation is similar to an email address and it is treated in this profile as of type String. This attribute is used in the context of the condor system to obtain, typically, a UID/GID or Username obligation. When this attribute is used, the other attributes do not need to be present. Vice versa, when this attribute is not used, the other attributes MUST be present, if known when composing the authorization request.

Requests containing a subject-condor-canonical-name-id MUST use the WN resource type and the “execute-now” action.

ID: subject-condor-canonical-name-id
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/subject-condor-canonical-name-id
XACML representation example:

```
<Attribute
 AttributeId="http://authz-interop.org/xacml/subject/subject-condor-canonical-name-id"
 DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>condor@fnal.gov</AttributeValue>
</Attribute>
```

6.1.4. Subject-x509-issuer

This attribute holds the Distinguished Name (DN) of the CA that signed the end entity user certificate. This DN is extracted from the user’s certificate and it is implicitly linked to the subject-x509 attribute-id. The datatype of this attribute is string, for the same reasons argued in the Subject-x509-id attribute.

ID: subject-x509-issuer
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/subject-x509-issuer
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/subject-x509-issuer"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth
   </AttributeValue>
</Attribute>
```

6.1.5. VO

This attribute holds the name of the first user Virtual Organization (VO) found in the set of attribute certificates. The user is requesting authorization in virtue of her membership to this VO,

project or community. There are two methods for extracting the VO name from an Attribute Certificate (AC): (1) from the “VO” attribute of the VOMS AC; (2) from the left-most slash-separated portion of the Fully Qualified Attribute Names (FQAN) [FQAN] attributes. This attribute contains the name extracted from the VO attribute of the AC (method 1).
From our experience multiple simultaneous VO usage has not observed the use case. All the VO specific attributes in VOMS (more of these will follow in the document) are describing the top VO which is represented explicitly in the VOMS-PRIMARY-FQAN attribute. The VOMS FQANs from all the potentially conveyed VOs CAN be expressed in the VOMS-FQAN attribute.

ID: vo
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/vo
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/vo"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>gin.ggf.org</AttributeValue>
</Attribute>
```

6.1.6. VOMS-signing-subject

VOMS-signing-subject holds the DN of the VOMS service that signed the first Attribute Certificate in the user credentials. It is extracted from the “issuer” attribute of the VOMS AC and is implicitly linked in this profile to the VOMS-signing-issuer attribute. As evident by its name, this attribute (and the others with similar names in this profile) is designed to convey information about an authoritative membership service implemented via a VOMS service. Other membership service implementations can still use this profile provided that their concepts can be properly described by the semantics of these attributes.

ID: voms-signing-subject
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/voms-signing-subject
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/voms-signing-subject"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>
     /O=dutchgrid/O=hosts/OU=nikhef.nl/CN=kuiken.nikhef.nl
   </AttributeValue>
</Attribute>
```

6.1.7. VOMS-signing-issuer

Considering that VOMS ACs are signed by a VOMS certificate, VOMS-signing-issuer holds the DN of the CA that signed that VOMS certificate. This attribute does not provide information about the whole trust chain: it provides only the DN of the CA that issued the first VOMS attribute certificate. VOMS-signing-issuer is implicitly linked in this profile to the VOMS-signing-subject attribute. It can be extracted programmatically using the VOMS API and is not displayed in typical command line tools, like voms-proxy-info.

ID: voms-signing-issuer

Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/voms-signing-issuer
XACML representation example:

```
<Attribute
    AttributeId="http://authz-interop.org/xacml/subject/voms-signing-issuer"
    DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth
   </AttributeValue>
</Attribute>
```

6.1.8. VOMS-FQAN

VOMS maintains the organizational structure of a VO in hierarchical *groups*. Users can belong to such *groups* and can have specific *roles* for each group. In the Attribute Certificate, the membership to a group with a role is encoded as a Fully Qualified Attribute Name (FQAN). This attribute holds one FQAN from the VOMS Attribute Certificate in the user credentials. Because users typically belong to several groups, this attribute can be set many times to encode all FQAN in the AC. For this profile, the order of the FQAN is not relevant, considering that the primary FQAN of the user is conveyed through the attribute VOMS-Primary-FQAN.
The PDP SHOULD perform a direct string match of the VOMS FQAN values when it evaluates an authorization request against its policy. VOMS FQANs have an optional suffix, e.g. /Role=NULL. A PDP COULD implement the VOMS matching rules to ignore these type of suffixes.

ID: voms-fqan
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/voms-fqan
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/voms-fqan"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>/gin.ggf.nl/APAC/Role=VO-Admin</AttributeValue>
</Attribute>
```

6.1.9. VOMS-Primary-FQAN

This attribute holds the FQAN that conveys the user's primary group to the middleware. Such primary group is chosen by the user when interacting with VOMS.
In OSG, the middleware uses this information to map the user credentials to an account group or account pool and, eventually, to a specific local account. This account is used for job scheduling and accounting to associate computing and data storage activities to the user's VO group and group role.
In EGEE, for computing activities, the middleware uses the primary FQAN to map the user credentials to a primary Unix Group ID (GID). The primary GID is used in batch system scheduling and in the accounting system to associate computing and data storage activities to VO groups and roles. For data management activities, the primary FQAN can be used to select one specific storage pool out of all the available VO storage pools.
This attribute is extracted from the topmost FQAN attribute of the Attribute Certificate list of FQAN. Therefore, this FQAN is also available in one of the VOMS-FQAN attributes of the XACML request (see description above). This duplication guarantees that the order of the foremost FQAN is maintained.

Note that not all the PDP require this information to take an authorization decision; therefore, if the value of this attribute is not set, the request is still valid. It is up to the PDP policy to accept or reject the authorization. Conversely, if multiple attributes are specified, only the first one SHOULD be used.

ID: voms-primary-fqan
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/voms-primary-fqan
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/primary-fqan"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>/gin.ggf.nl/APAC/Role=VO-Admin</AttributeValue>
</Attribute>
```

6.1.10. Certificate-serial-number

This attribute holds the serial number of the user certificate. This attribute is of type integer. It is extracted from the user certificate.
This attribute can be used by a site to centrally blacklist a compromised certificate before the Certificate Revocation Lists from the CA are distributed to all gateways at a site.
This attribute is considered optional because the CA is responsible for conducting the investigation on whether to revoke a certificate. If the certificate needs to be revoked, sites expect that the CA takes immediate action, entering the certificate in the CRL.

ID: certificate-serial-number
Type: integer
Full Attribute ID: http://authz-interop.org/xacml/subject/certificate-serial-number
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/certificate-serial-number"
   DataType="http://www.w3.org/2001/XMLSchema#integer">
  <AttributeValue>28</AttributeValue>
</Attribute>
```

6.1.11. Validity-not-before

In order for PDPs to enforce policies on the time length of validity of a certificate chain, the profile allows to send validity not-before and not-after dates for the chain. A site, for example, might want to define an authorization policy that rejects proxies with a lifetime longer than a week. These attributes are of type dateTime. The values are extracted by iterating over the certificate chain and extracting the most recent past validity not-before date and the most immediate future validity not-after date. For well formed certificates, these should be equivalent to the not-before and not-after dates of the file proxy in the chain.
The time is expressed in UTC time zone.

ID: validity-not-before
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/validity-not-before
XACML representation example:

```
<Attribute
   AttributeId=”http://authz-interop.org/xacml/subject/validity-not-before”
   DataType=”http://www.w3.org/2001/XMLSchema#dateTime”>
   <AttributeValue>2011-07-27T18:41:54Z</AttributeValue>
</Attribute>
```

6.1.12. Validity-not-after

See Validity-not-before attribute for an explanation of this attribute.

ID: validity-not-after
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/validity-not-after
XACML representation example:

```
<Attribute
    AttributeId=”http://authz-interop.org/xacml/subject/validity-not-after”
    DataType=”http://www.w3.org/2001/XMLSchema#dateTime”>
    <AttributeValue>2011-07-28T06:46:54Z</AttributeValue>
</Attribute>
```

6.2. Optional Subject Attributes

The following attributes are considered optional to this profile and allow for implementation specific policies which extend an authorization decision based on X.509, VOMS FQANs or POSIX credentials. . They are discussed here to reserve the attribute names for a possible future use.

6.2.1. CA-serial-number

This attribute holds the CA’s serial number used to sign the user certificate. The DN of such CA is the subject-issuer. The CA’s serial number CAN be extracted from the CA certificate.
Sites can use this information to blacklist a compromised CA before the CA certificate is revoked. This attribute gives a finer grained blacklisting capability than the CA DN. In fact, a CA can re-issue a new certificate, with a different serial number by design, but with the same DN as the compromised CA certificate. Blacklisting the DN would not allow to ban the compromised CA and accept the new CA, until the compromised CA certificate is in the Certificate Revocation List.
This attribute is considered optional because sites trust the CA to include the compromised CA certificate in the Certificate Revocation List before issuing a new CA certificate.

ID: ca-serial-number
Type: integer
Full Attribute ID: http://authz-interop.org/xacml/subject/ca-serial-number
XACML representation example:

```
<Attribute
   AttributeId http://authz-interop.org/xacml/subject/ca-serial-number"
   DataType="http://www.w3.org/2001/XMLSchema#integer">
   <AttributeValue>34</AttributeValue>
</Attribute>
```

6.2.2. VOMS-dns-port

This attribute holds the DNS name of the host and the port number of the VOMS server that signed the VOMS ACs. The format of the value represents the string concatenation of the hostname as Fully Qualified Domain Name (FQDN), a separator in the form of a colon and the TCP port number.
This attribute is considered optional because it is not currently used by any authorization middleware from our group.

ID: voms-dns-port
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/voms-dns-port
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/voms-dns-port"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>kuiken.nikhef.nl:15050</AttributeValue>
</Attribute>
```

6.2.3. Subject End-Entity X509v3 Certificate Policies OIDs

This attribute holds active Certificate Policy OIDs for the certificate of the subject. These values are extracted from the user certificate. These values originate from the CA and give additional information about the certificate; for example, it allows distinguishing between user, host, service, and robot certificates. There can be multiple of these attributes set in one request.
This attribute is considered optional because it is not currently used by any authorization middleware from our group.

ID: ca-policy-oid
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/ca-policy-oid
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/subject/ca-policy-oid"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>1.2.840.113612.5.2.4</AttributeValue>
</Attribute>
```

6.2.4. Certificate Chain

This attribute holds the certificate chain of the subject-id. This can provide the opportunity to centrally verify the certificate chain. This would eliminate the need for having CA certificates, CRLs, and VOMS signing certificates managed at all PEP nodes. In addition, the load at the resource gateways will be lowered with a central validation approach. This attribute allows also deeper inspection of the whole chain, beyond the attributes explicitly conveyed by this profile.
The value type of this attribute is a string containing a Base64 binary representation of the certificate. This attribute is considered optional because it is not currently used by any authorization middleware from our group.

ID: cert-chain
Type: string
Full Attribute ID: http://authz-interop.org/xacml/subject/cert-chain

XACML representation example:

```
<Attribute
    AttributeId="http://authz-interop.org/xacml/subject/cert-chain"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>-----BEGIN CERTIFICATE-----
MIICbjCCAVagAwIBAgICBNgwDQYJKoZIhvcNAQEEBQAwTDESMBAGA1UEChMJZHV0
Y2hncmlkMQ4wDAYDVQQKEwV1c2VyczEPMA0GA1UEChMGbmlraGVmMRUwEwYDVQQD
EwxPc2NhciBLb2Vyb28wHhcNMDcxMTEzMTM0MjU4WhcNMDcxMTE0MDE0NzU4WjBc
MRIwEAYDVQQKEwlkdXRjaGdyaWQxDjAMBgNVBAoTBXVzZXJzMQ8wDQYDVQQKEwZu
aWtoZWYxFTATBgNVBAMTDE9zY2FyIEtvZXJvbzEOMAwGA1UEAxMFcHJveHkwXDAN
BgkqhkiG9w0BAQEFAANLADBIAkEAs1EsIXp1WQeL3X52VTvmT1a2XTP5DuCgov6w
dhKWdYL/KPA/wj12HXBNvF/1ZI+09TZPJC/IDnjnMPxp3bzvOwIDAQABoxIwEDAO
BgNVHQ8BAf8EBAMCBLAwDQYJKoZIhvcNAQEEBQADggEBAE4+PkN9ClrmtldmNAHE
EBcKobYiZie8vvNMPNWiXs5BgeoYHmMvkyXBi6JSrDy1FoMID96LROmncc4fI2N7
CxxaLKXO0GFpxEfWKeaSAaU5KyTyCSozqdj5MGHAid9juB4RtHqh2hTKN+akma1X
RWQ22pxzUL/iIZ26Kn78Yv0cbytE/1reg3F8Y8txj4VHOypBFTLke/zM44xajH+z
/i8QrPcLqwqpvLLjf3gXaT2JKAKjTDisArefkPDLSStXDUc2qv04RMK1wXbhc+J8
3Qe6b/hOuPNur5D9mQvH4tvGwDtphKMy1hrfY39ATxViKoZ/gkSOeihFCLPC8dbR
zm0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFQzCCBCugAwIBAgICBNgwDQYJKoZIhvcNAQEFBQAwUjELMAkGA1UEBhMCTkwx
DzANBgNVBAoTBk5JS0hFRjEyMDAGA1UEAxMpTklLSEVGIG1lZGl1bS1zZWN1cml0
eSBjZXJ0aWZpY2F0aW9uIGF1dGgwHhcNMDcwMTIzMDAwMDAwWhcNMDgwMTIzMTY1
NDA1WjBMMRIwEAYDVQQKEwlkdXRjaGdyaWQxDjAMBgNVBAoTBXVzZXJzMQ8wDQYD
VQQKEwZuaWtoZWYxFTATBgNVBAMTDE9zY2FyIEtvZXJvbzCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALOut6/xkQ4d4iZhXahraVE9ZAGy9u5vnPD0NXfS
fJC6YxPf3NpQy1rCDVXXCgkP0DOj4Jeb7o/vpwpNwciPo/zcaQjlCOBJf5oOSXvO
O9TqnwafkypQVthIvpSvcUK+LX0aHUB+VmphZF2UCi5Ai0HkqZgDo+rx0cikVQme
mKFUQfuY9EfQlDrIgL1pGswW0IEZ5XSnb9EkHWS0xT6TOzwItIftvlNqV/9gr1P+
W+H+nqu+k+k7ouYlSnME7HK8OgneBZZj4A452OTKlPoW8BB4HMW1ISekUme0imNJ
Zt+T1AJKSl3wCRj5SG3FIbC8Y4Y5AnOBCJfd99Kw6lAGXW8CAwEAAaOCAicwggIj
MAwGA1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgTwMDgGA1UdHwQxMC8wLaAroCmG
J2h0dHA6Ly9jYS5kdXRjaGdyaWQubmwvbWVkaXVtL2NhY3JsLnBlbTAaBgNVHSAE
EzARMA8GDSsGAQQB0UIEAgIBAgIwegYDVR0jBHMwcYAUWwU6mcbVIr39lID8EajQ
8XHWS6ShVqRUMFIxCzAJBgNVBAYTAk5MMQ8wDQYDVQQKEwZOSUtIRUYxMjAwBgNV
BAMTKU5JS0hFRiBtZWRpdW0tc2VjdXJpdHkgY2VydGlmaWNhdGlvbiBhdXRoggEA
MB0GA1UdDgQWBBRMgdE9QZSl7SOfCMk1q6Uw0sGoSjARBglghkgBhvhCAQEEBAMC
BeAwNAYJYIZIAYb4QgEIBCcWJWh0dHA6Ly9jYS5kdXRjaGdyaWQubmwvbWVkaXVt
L3BvbGljeS8wgcgGCWCGSAGG+EIBDQSBuhaBt0NlcnRpZmljYXRlIGlzc3VlZCB1
bmRlciBEdXRjaEdyaWQgbWVkaXVtLXNlY3VyaXR5IHBvbGljeSB2ZXJzaW9uIDIu
MjtsaW1pdGVkIGxpYWJpbGl0aWVzIGFwcGx5LCBzZWUgaHR0cDovL2NhLmR1dGNo
Z3JpZC5ubC9tZWRpdW0vcG9saWN5LyBmb3IgZGV0YWlsesztDZXJ0aWZpY2F0ZSBU
YWc6IGVkMGExM2E0LWIzYWViNzANBgkqhkiG9w0BAQUFAAOCAQEAdRzg6tOX6ZwB
CthL7NSPSFzpVeIVcBnQCuXRBANIoPf3fSOBEyKt49cJfCeZywCdPEJe/vzsatjX
+zNfz+KBMTJ449neIekY+0xh8XR2sIVNgqjP0+5qkyBXbIQSLZnOk6OI5XAWlpKy
YMp89wdk515cPJhTx65+IerO7yN7feotW6KtkxMLU/Fs77EmwoPj+c0E2VAVAZfP
AZ8xiCNFGgpzPFHAtCngSjwjoUiOFd4v+4fia18V4lFcNt1lhnaQZ6x832YYhDO9
1i791ebCBw2prcrwHOy5JEgdswG8QymBd+7dv7wl3gebI3a/Oq+OmNa/RiL3SKPx
dgfW33EuFg==
-----END CERTIFICATE-----</AttributeValue>
</Attribute>
```

6.3. Action

The attributes in the Action context describe what action the subject wants to perform on the specified resource. In this profile, we have kept the accepted actions to a minimum. To do this, we have abstracted specific actions in single generic actions; for example, all interactions with the job queue of a batch system exposed through a standard Grid interface (i.e. a Computing Element - CE) is described by a single action named “queue”, which generalizes possible “queuing” actions like “submit-job”, “delete-job”, “query-job-status”, etc. In addition, we use generalized actions for different types of resources, when possible: for example, the action “execute-now” applies to both Computing Eelement and Worker Node (WN) resources. We encourage these generalizations for future extensions to this profile. It should be notes that we do

not attempt to prescribe any mechanisms for the extension of this profile, including the use of a registrar or specific use cases, such as deeper queries (e.g. /queue/query or /queue/list). In our reference implementation, all actions are compared against policies for an “exact match” only.

We consider 3 types of actions. Their names are “queue”, “execute-now” and “access”, with prefix *<action-prefix>/action-type/*. A request defines a certain action by setting the value of the attribute name “action-id” to one of these 3 types of action names.

6.3.1. Namespace Prefix Expansion

By concatenation with the URL root-prefixes, the namespace prefix of action attributes (action-prefix) is expanded to the following prefix:

URL based namespace prefix: <URL root prefix> + "/action"

6.3.2. Queue: Action Type - Access a Job Queue

The “queue” action states that the subject requests authorization to interact with the job queue of the specified computing resource. The queue name, if available, CAN be extracted from the Resource Specification Language (RSL) string attribute of the action context (see below).
This action is used in conjunction with the CE resource type, typically when requesting authorization to submit a job to the batch system queue controlled by a CE.
As defined, this action CAN be used also to request authorization to monitor a remote queue. Because of our use cases, we make no attempt to allow a policy distinction between the immutable (monitoring) and the mutable (job queuing) action.
Note that action-id is a standardized attribute and it is left in URN notation.

ID: action-id
Type: string
Full Attribute ID: urn:oasis:names:tc:xacml:1.0:action:action-id
ID Value: http://authz-interop.org/xacml/action/action-type/queue
Enumeration of possible values:
http://authz-interop.org/xacml/action/action-type/queue
http://authz-interop.org/xacml/action/action-type/execute-now
http://authz-interop.org/xacml/action/action-type/access
XACML representation example:

```
<Attribute
    AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://authz-interop.org/xacml/action/action-type/queue
    </AttributeValue>
</Attribute>
```

6.3.3. Execute-now: Action Type - Run Job Now

The “execute-now” action states that the subject requests authorization to execute immediately a job at the specified computing resource (e.g. for a typical CE, invoking the job-manager fork of a Globus gatekeeper). This action is in contrast to the “queue” action, typically used for submitting a job to a batch system queue.
Requests to a PDP containing a subject-condor-canonical-name-id SHOULD use the WN resource type and the “execute-now” action.
Note that action-id is a standardized attribute and it is left in URN notation.

ID: action-id
Type: string
Full Attribute ID: urn:oasis:names:tc:xacml:1.0:action:action-id
ID Value: http://authz-interop.org/xacml/action/action-type/execute-now
Enumeration of possible values:
http://authz-interop.org/xacml/action/action-type/queue
http://authz-interop.org/xacml/action/action-type/execute-now
http://authz-interop.org/xacml/action/action-type/access
XACML representation example:

```
<Attribute
   AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>http://authz-interop.org/xacml/action/action-type/execute-now
   </AttributeValue>
</Attribute>
```

6.3.4. Access: Action Type - Access a Storage Resource

The “access” action states that the subject requests authorization to access a specified storage resource. The scope of the request is implementation dependent: the request CAN regard access to a single file, a list of files, a remote/local storage pool, or an entire storage system.
By design, this action generalizes finer-grain types of access, like read access, write access, file system administrative access, etc. Such fine grained access control should be delegated to the authorization layer of storage services. In fact, centralizing such control in the PDP is considered too costly in terms of performance. In addition, administrators typically are already comfortable with the authorization layers of their storage services and we see little benefit in proposing alternatives to such mechanisms.
Note that action-id is a standardized attribute and it is left in URN notation.

ID: action-id
Type: string
Full Attribute ID: urn:oasis:names:tc:xacml:1.0:action:action-id
ID Value: http://authz-interop.org/xacml/action/action-type/access
Enumeration of possible values:
http://authz-interop.org/xacml/action/action-type/queue
http://authz-interop.org/xacml/action/action-type/execute-now
http://authz-interop.org/xacml/action/action-type/access
XACML representation example:

```
<Attribute
   AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id "
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>http://authz-interop.org/xacml/action/action-type/access
   </AttributeValue>
</Attribute>
```

6.3.5. Resource Specification Language Attribute: rsl-string

This attribute holds a string describing additional details of the action to be performed on the resource. This attribute is mainly thought to be used for actions performed on a CE resource, where such additional details can be described by a Globus Resource Specification Language

[RSL] string. This string can hold information such as the name of the batch system queue targeted for job submission, the expected maximum running wall clock time for the job, etc.

ID: rsl-string
Type: string
Full Attribute ID: http://authz-interop.org/xacml/action/rsl-string
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/action/rsl-string"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue> (jobtype='single')(maxtime=1100)(queue='hep')</AttributeValue>
</Attribute>
```

6.4. Resource

The attributes in the Resource context describe the resource targeted for the authorization request. In this profile, we define only resources of particular interest to our community. We acknowledge that this is not a complete list and we encourage the extension of this section in future editions of this document.
In this context, we also define resource attributes useful for the authorization request, such as the DNS name of the machine hosting the gateway service to the resource and the X509 certificate information of that gateway service.

We consider three types of resources. Their names are “ce”, “wn” and “se”, with prefix *<resource-prefix>/resource-type/*. A request targets a certain resource by setting the value of the attribute name “resource-id” to one of these 3 types of resource name.

6.4.1. Namespace Prefix Expansion

By concatenation with the URL root-prefixes, the namespace prefix of resource attributes is expanded to the following prefix:

URL based namespace prefix: <URL root prefix> + "/resource-type"

6.4.2. CE: Resource Type - Computing Element

The Computing Element resource manages the execution of jobs on underlying computing resources. The CE is responsible for interacting with the PDP before granting access to the job queuing system of its underlying computing cluster (“queue” action) or to the local machine execution environment (“execute-now” action).
Note that resource-id is a standardized attribute and it is left in URN notation.

ID: resource-id
Type: string
Full Attribute ID: urn:oasis:names:tc:xacml:1.0:resource:resource-id
ID Value: http://authz-interop.org/xacml/resource/resource-type/ce
Enumeration of possible values:
http://authz-interop.org/xacml/resource/resource-type/ce
http://authz-interop.org/xacml/resource/resource-type/se
http://authz-interop.org/xacml/resource/resource-type/wn
XACML representation example:

```
<Attribute
   AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>http://authz-interop.org/xacml/resource/resource-type/ce
   </AttributeValue>
</Attribute>
```

6.4.3. WN: Resource Type - Worker Node

A Worker Node is a machine of a computing cluster. The Worker Node resource manages the execution of jobs on the local machine execution environment.
Job executions on WNs may or may not require an authorization decision initiated by a WN, depending on the job management model used. In a push-based job management model, WN authorization is not required: jobs are submitted to a CE, where the authorization request is issued, and then dispatched to the WN via the local batch system. In a pull-based job management model, WN authorization is required: special jobs, referred to as pilot jobs, are dispatched to the WN using a push-based model; once pilot jobs start execution, they pull a user job workload from a VO repository. To protect the execution environment, the WN issues an authorization request for the user workload; if granted, the workload is executed with the privileges locally assigned to that user. The authorization request initiated by the WN MUST use the action “execute-now”.
Requests to a PDP containing a subject-condor-canonical-name-id SHOULD use the WN resource type and the “execute-now” action.
Note that resource-id is a standardized attribute and it is left in URN notation.

ID: resource-id
Type: string
Full Attribute ID: urn:oasis:names:tc:xacml:1.0:resource:resource-id
ID Value: http://authz-interop.org/xacml/resource/resource-type/wn
Enumeration of possible values:
http://authz-interop.org/xacml/resource/resource-type/ce
http://authz-interop.org/xacml/resource/resource-type/se
http://authz-interop.org/xacml/resource/resource-type/wn
XACML representation example:

```
<Attribute
    AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://authz-interop.org/xacml/resource/resource-type/wn
    </AttributeValue>
</Attribute>
```

6.4.4. SE: Resource Type - Storage Element

The Storage Element resource manages access to files and storage pools. Authorization requests to storage elements MUST use the action “access”.
Note that resource-id is a standardized attribute and it is left in URN notation.

ID: resource-id
Type: string
Full Attribute ID: urn:oasis:names:tc:xacml:1.0:resource:resource-id
ID Value: http://authz-interop.org/xacml/resource/resource-type/se

Enumeration of possible values:
http://authz-interop.org/xacml/resource/resource-type/ce
http://authz-interop.org/xacml/resource/resource-type/se
http://authz-interop.org/xacml/resource/resource-type/wn
XACML representation example:

```
<Attribute
    AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://authz-interop.org/xacml/resource/resource-type/se
    </AttributeValue>
</Attribute>
```

6.4.5. Host DNS name: dns-host-name

This attribute specifies the fully qualified domain name of the machine hosting the gateway to the specified resource. Examples of such gateway include a Globus Gatekeeper, for the CE; SRM, for the SE; gLExec, for the WN.
This attribute is of type string.

ID: dns-host-name
Type: string
Full Attribute ID: http://authz-interop.org/xacml/resource/dns-host-name
XACML representation example:

```
<Attribute
    AttributeId="http://authz-interop.org/xacml/resource/dns-host-name"
    DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>ce03.nikhef.nl</AttributeValue>
</Attribute>
```

6.4.6. Resource X509 Service Certificate Subject: resource-x509-id

This attribute specifies the X509 subject of the service certificate that defines the identity of the resource gateway. This certificate is typically the host certificate of the machine hosting the gateway, but it CAN be a generic service certificate. If the information of this service certificate is available to the PEP authorization environment, this information MUST be included in the request.
This attribute is of type string, instead of X.500, for the same reasons discussed in the subject-x509-id attribute section.

ID: resource-x509-id
Type: string
Full Attribute ID: http://authz-interop.org/xacml/resource/resource-x509-id
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/resource/resource-x509-id"
   DataType="http://www.w3.org/2001/XMLSchema#string">
  <AttributeValue>/DC=org/DC=doegrids/OU=Services/CN=my.host.domain</AttributeValue>
</Attribute>
```

6.4.7. Resource X509 Service Certificate Issuer: resource-x509-issuer

This attribute specifies the X509 issuer of the service certificate that defines the identity of the resource gateway. This attribute identifies the CA that signed the service certificate for the resource gateway. If the information of this service certificate is available to the PEP authorization environment, this information MUST be included in the request.
This attribute is of type string, instead of X.500, for the same reasons discussed in the subject-x509-id attribute section.

ID: resource-x509-issuer
Type: string
Full Attribute ID: http://authz-interop.org/xacml/resource/resource-x509-issuer
XACML representation example:

```
<Attribute
   AttributeId="http://authz-interop.org/xacml/resource/resource-x509-issuer"
   DataType="http://www.w3.org/2001/XMLSchema#string">
   <AttributeValue>/DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
   </AttributeValue>
</Attribute>
```

6.5. Environment

The attributes in the Environment context convey additional parameters in the authorization request of the subject to perform an action on the specified resource. These additional parameters instruct the PDP on what obligations the PEP supports or convey information about the pilot job identity in case of authorization requests initiated by a WN.

6.5.1. Namespace prefix expansion

By concatenation with the URL root-prefixes, the namespace prefix of environment attributes is expanded to the following prefix:

URL based namespace prefix: <URL root prefix> + "/environment"

6.5.2. Supported Obligations

PDPs encapsulate in obligation structures the set of constraints that a PEP MUST be able to satisfy before granting access to resources. Obligations are identified by an obligation id, which typically PEPs associate to obligation handler code. According to the XACML specifications, even if only one obligation cannot be satisfied by the PEP, the authorization MUST be denied. A PEP may not be able to satisfy an obligation because it does not know how to act upon it i.e. it does not have an appropriate handler for a certain obligation-id. Such situation may occur especially during upgrades of PDP servers, potentially resulting in the PEP receiving new and unknown obligations, thus having to reject all authorization requests.
In order to mitigate such a problem, this profile allows for a PEP to specify the list of known obligations via the XACML environment context. A PDP CAN take such list under advisement and deal with a version compatibility problem by returning a set of obligations appropriate for the PEP. On the other hand, it should be noted that a PDP CAN elect to ignore the list of supported obligations and still be compliant with this profile.

The example below shows how a PEP uses the XACML environment context to communicate the list of obligations supported to a PDP.

ID: pep-oblig-supported
Type: string
Full Attribute ID: http://authz-interop.org/xacml/environment/pep-oblig-supported
ID Value: a valid obligation ID (see Obligations section)
Enumeration of possible values:
http://authz-interop.org/xacml/obligation/uidgid
http://authz-interop.org/xacml/obligation/secondary-gids
http://authz-interop.org/xacml/obligation/username

http://authz-interop.org/xacml/obligation/root-and-home-paths
http://authz-interop.org/xacml/obligation/storage-access-priority
http://authz-interop.org/xacml/obligation/access-permissions
Notes: This attribute may appear multiple times, each time with a different value (as many times as supported obligations)
XACML representation example:

```
<Attribute
    AttributeId="http://authz-interop.org/xacml/environment/pep-oblig-supported"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://authz-interop.org/xacml/obligation/uidgid
    </AttributeValue>
</Attribute>

<Attribute
    AttributeId="http://authz-interop.org/xacml/environment/pep-oblig-supported"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://authz-interop.org/xacml/obligation/secondary-gids
    </AttributeValue>
</Attribute>

<Attribute
    AttributeId="http://authz-interop.org/xacml/environment/pep-oblig-supported"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>http://authz-interop.org/xacml/obligation/username
    </AttributeValue>
</Attribute>
```

6.5.3. Pilot Job Invoker Identity

The pull-based job management model can be summarized as follows. Special jobs, named “pilot” jobs, are submitted to to Computing Elements. These jobs are authorized by the CE to access computing resources and are eventually dispatched to Worker Nodes via the local batch system. Once one such job runs at a Worker Node, it pulls a user workload from a VO repository. Such workload needs to be executed with the privileges of the user, not the privileges of the pilot. The WN can request authorization for the user to access the local WN execution environment and, if granted, execute the job under user privileges.
In this scenario, the authorization request conveys user identity information in the subject context, WN information (typically WN host certificate) in the resource context, and pilot job identity information in the environment context. Such information is important to enforce various policies on pilot job scenarios. An example of such a policy states that user access to the WN execution

environment should be granted only if the pilot job belongs to the same VO of the user. With the information provided in this profile, such policy can be expressed and enforced.

The pilot job identity is expressed as a set of flat attributes in the environment context. All attributes specified in the subject context MUST be defined for the pilot identity in the environment context. Pilot attributes have the same attribute id of the subject attributes with different namespace:

```
<URL root prefix> + "/environment" + "/pilot-job"
```

Attributes that define the user identity in the subject context have the same meaning of the attributes that define the pilot identity in the environment context.
Authorization requests for an action “execute-now” on a resource “WN” MUST have pilot job identity information, unless the request contains a subject-condor-canonical-name-id attribute.

For a full list of attributes see the environment section in “Appendix B: List of Attribute and Obligation IDs introduced by this profile”.

7. XACML Response

The following section defines the authorization interoperability attributes for the XACML response message. It defines obligations and attributes for the obligations context.

7.1. Obligations

The following is the list of obligations in this profile. Each obligation has an ID, a list of attributes, corresponding types, and a stakeholder (EGEE, VO Services project, …). The types are chosen from the available datatypes in the XML Schema [XMLSchema]. This document also captures if an obligation requires the presence of another to make sense in our use cases. These dependencies will not be captured in a structured way in the protocol. It is up to the PEP that receives the message to validate these dependencies.
The combination of attributes in each of the described obligations is tuned to the use cases that are common to Grid systems. Attributes that cannot be useful separately are bound together in one obligation. Other attributes are split in different obligations because they can be combined in a response that is use case-dependent.

7.2. Namespace prefix expansion

By concatenation with the URL URN root-prefixes, the namespace prefix of obligations is expanded to the following prefix:

URL based namespace prefix: <URL root prefix> + "/obligation"

The namespace prefix of attributes is expanded to the following prefix:

URL based namespace prefix: <URL root prefix> + "/attribute"

7.3. UID GID

This obligation requires that the resource gateway (PEP) creates an execution environment for the user with a specific Unix ID (UID) and Group ID (GID). If this obligation is received together with the username obligation, the two must be consistent i.e. the UID attribute from the uidgid obligation must be mapped to the given UNIX username and vice versa. If this is NOT the case, the authorization MUST be denied.

ID: uidgid
Full Obligation ID: http://authz-interop.org/xacml/obligation/uidgid
Attributes:
ID: posix-uid
Description: Unix User ID local to the PEP
Type: integer
Full Attribute ID: http://authz-interop.org/xacml/attribute/posix-uid

ID: posix-gid
Description: Unix Group ID local to the PEP
Type: integer
Full Attribute ID: http://authz-interop.org/xacml/attribute/posix-uid
Stakeholder: Common

Must be consistent with: Username
XACML representation example:

```
<Obligation ObligationId="http://authz-interop.org/xacml/obligation/uidgid"
   FulfillOn="Permit">
   <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/posix-uid"
    DataType="http://www.w3.org/2001/XMLSchema#integer">
       7160
   </AttributeAssignment>

   <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/posix-gid"
    DataType="http://www.w3.org/2001/XMLSchema#integer">
      1530
  </AttributeAssignment>
</Obligation>
```

7.4. Multiple Secondary GIDs

This obligation requires that the PEP sets secondary Unix Group IDs when creating the execution environment. The list of GIDs MAY be empty. This obligation is typically used in conjunction with UIDGID. The main use case for this obligation is to take full advantage of the Unix file permissions. This is needed to facilitate fine-grain access to specific storage areas.

ID: secondary-gids
Full Obligation ID: http://authz-interop.org/xacml/obligation/secondary-gids
Attributes:
ID: posix-gid
Description: Unix Group ID local to the PEP
Type: integer
Notes: this attribute can appear multiple times within this obligation
Full Attribute ID: http://authz-interop.org/xacml/attribute/posix-gid
Stakeholder: EGEE/EMI
Needs obligation(s): uidgid

XACML representation example:

```
<Obligation ObligationId="http://authz-interop.org/xacml/obligation/secondary-gids"
   FulfillOn="Permit">
  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/posix-gid"
    DataType="http://www.w3.org/2001/XMLSchema#integer">
      1531
  </AttributeAssignment>
  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/posix-gid"
    DataType="http://www.w3.org/2001/XMLSchema#integer">
      1530
  </AttributeAssignment>
</Obligation>
```

7.5. Username

This obligation requires that the PEP sets the UNIX username, passed as a string, for the execution environment. If this obligation is received together with the uidgid obligation, the two must be consistent i.e. the UID attribute from the UIDGID obligation must be mapped to the given UNIX username and vice versa. If this is not the case, the authorization MUST be denied.

ID: username
Full Obligation ID: http://authz-interop.org/xacml/obligation/username
Attributes:
ID: username
Description: Unix username or account name local to the PEP.
Type: string
Full Attribute ID: http://authz-interop.org/xacml/attribute/username
Stakeholder: VO Services Project
Must be consistent with: uidgid
XACML representation example:

```
<Obligation ObligationId="http://authz-interop.org/xacml/obligation/username"
   FulfillOn="Permit">
  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/username"
    DataType="http://www.w3.org/2001/XMLSchema#string">
      garzoglio
  </AttributeAssignment>
</Obligation>
```

7.6. Path Restriction

This obligation requires that the PEP restricts access to the file system from the execution environment. In particular, it defines a sub-tree of the file system (RootPath) that should be the "root" mount point of the execution environment (i.e. '/') and it defines the path to the user's home directory (HomeDir), as a subpath of the RootPath. This obligation is mostly used to control access privileges to storage elements and it is typically used in conjunction with UIDGID or Username.

ID: root-and-home-paths
Full Obligation ID: http://authz-interop.org/xacml/obligation/root-and-home-paths
Attributes:
ID: rootpath
Description: this parameter defines a sub-tree of the whole file system available at the PEP. The PEP should mount this sub-tree as the "root" mount point ('/') of the execution environment. This is an absolute path.
Type: string
Full Attribute ID: http://authz-interop.org/xacml/attribute/rootpath

ID: homepath
Description: this parameter defines the path to home areas of the user accessing the PEP. This is a path relative to rootpath.
Type: string
Full Attribute ID: http://authz-interop.org/xacml/attribute/homepath

Stakeholder: VO Services Project
Needs obligation(s): uidgid or username
XACML representation example:

```
<Obligation ObligationId="http://authz-interop.org/xacml/obligation/root-and-home-paths"
   FulfillOn="Permit">
  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/rootpath"
    DataType="http://www.w3.org/2001/XMLSchema#string">
      /pnfs/myvo/
  </AttributeAssignment>

  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/homepath"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <!-- Set the home path to /pnfs/myvo/home/garzoglio -->
      home/garzoglio/
  </AttributeAssignment>
</Obligation>
```

7.7. Storage Priorities

This obligation requires that the PEP provides access to storage resources with a priority indicated by the integer parameter passed via the obligation. The higher the integer value, the higher the priority. A priority is related to the position of the request in the data request queue. This obligation is typically used in conjunction with UIDGID or Username.

ID: storage-access-priority
Full Obligation ID: http://authz-interop.org/xacml/obligation/storage-access-priority
Attributes:
ID: storage-priority
Description: an integer number that defines the priority to access storage resources.
Type: integer
Full Attribute ID: http://authz-interop.org/xacml/attribute/storage-priority
Stakeholder: VO Services Project
Needs obligation(s): uidgid or username
XACML representation example:

```
<Obligation ObligationId="http://authz-interop.org/xacml/obligation/storage-access-
priority"
   FulfillOn="Permit">
  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/storage-priority"
    DataType="http://www.w3.org/2001/XMLSchema#integer">
      10
  </AttributeAssignment>
</Obligation>
```

7.8. Access Permission

This obligation requires that the PEP provide access to the storage resources in read-only or read-write modes. This obligation is typically used in conjunction with UIDGID or Username.

Further finer-grain restrictions can be applied as POSIX permissions by the storage service when accessing individual files.

ID: access-permissions
Full Obligation ID: http://authz-interop.org/xacml/obligation/access-permissions
Attributes:
ID: access-permissions
Description: a string that represent the access permission to a file that is requested. This attribute can have values “read-only” or “read-write”.
Type: string
Full Attribute ID: http://authz-interop.org/xacml/attribute/access-permissions
Stakeholder: VO Services Project
Needs obligation(s): uidgid or username
XACML representation example:

```
<Obligation ObligationId="http://authz-interop.org/xacml/obligation/access-permissions"
   FulfillOn="Permit">
  <AttributeAssignment
    AttributeId="http://authz-interop.org/xacml/attribute/access-permissions"
    DataType="http://www.w3.org/2001/XMLSchema#string ">
      read-only
  </AttributeAssignment>
</Obligation>
```

8. Appendix A: Example Response / Request messages and corresponding XACML Policies

8.1. A.1 Example of simple Request/Response and Policy

a) Simple Request message that contains information about requesting Subject, Resource, Action

```
[1]  <Request
[2]        xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
[3]        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[4]        xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
[5]          access_control-xacml-2.0-context-schema-os.xsd">
[6]    <!-- Example - Request: Simple Request-Policy-Response -->
[7]    <Subject>
[8]      <Attribute
[9]            AttributeId="http://authz-interop.org/xacml/subject/subject-x509-id"
[10]           DataType="http://www.w3.org/2001/XMLSchema#string">
[11]       <AttributeValue>/O=dutchgrid/O=users/O=nikhef/CN=Wim
Huizinga</AttributeValue>
[12]     </Attribute>
[13]     <Attribute
[14]           AttributeId="http://authz-interop.org/xacml/subject/subject-x509-
issuer"
[15]           DataType="http://www.w3.org/2001/XMLSchema#string">
[16]       <AttributeValue>/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification
auth</AttributeValue>
[17]     </Attribute>
[18]     <Attribute
[19]           AttributeId="http://authz-interop.org/xacml/subject/vo"
[20]           DataType="http://www.w3.org/2001/XMLSchema#string">
[21]       <AttributeValue>gin.ggf.nl</AttributeValue>
[22]     </Attribute>
[23]     <Attribute
[24]           AttributeId="http://authz-interop.org/xacml/subject/voms-primary-fqan"
[25]           DataType="http://www.w3.org/2001/XMLSchema#string">
[26]       <AttributeValue>/gin.ggf.nl/APAC/Role=Researcher</AttributeValue>
[27]     </Attribute>
[28]   </Subject>
[29]   <Resource>
[30]     <Attribute
[31]          AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
[32]          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
[33]       <AttributeValue>http://authz-interop.org/xacml/resource/resource-
type/se</AttributeValue>
[34]     </Attribute>
[35]   </Resource>
```

```
[36]  <Action>
[37]    <Attribute
[38]         AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[39]         DataType="http://www.w3.org/2001/XMLSchema#string">
[40]       <AttributeValue>http://authz-interop.org/xacml/action/action-
type/access</AttributeValue>
[41]    </Attribute>
[42]  </Action>
[43]  <Environment/>
[44]</Request>
```

b) Response message with returned obligations in lines [53-58] to map user identity to returned UID and GID under which the user task/request will be executed.

```
[45]<?xml version="1.0" encoding="UTF-8"?>
[46]<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[47]xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
access_control-xacml-2.0-context-schema-os.xsd">
[48]  <Result ResourceId=" http://authz-interop.org/xacml/resource/resource-type/se">
[49]    <Decision>Permit</Decision>
[50]    <Status>
[51]<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
[52]    </Status>
[53]    <xacml:Obligations>
[54]<xacml:Obligation ObligationId="http://authz-interop.org/xacml/obligation/uidgid"
FulfillOn="Permit">
[55]<xacml:AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-uid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2501</xacml:AttributeAssignment>
[56]<xacml:AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-gid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2101</xacml:AttributeAssignment>
[57]</xacml:Obligation>
[58]  </xacml:Obligations>
[59]  </Result>
[60]</Response>
```

c) Example policy with obligations in lines [113-118].

- Policy Target in lines [71-90] provides conditions by which policy is selected based on information in the Request message: Subject VO and Resource
- Rule Target in lines [95-104] specifies action for which the rule is applied.

Condition expression in lines [106-110] uses bag-function to specify that any of the Subject attributes with AittributeId="…/voms-fqan" should match value "/gin.ggf.nl/APAC/Role=Researcher"

```
[61]<?xml version="1.0" encoding="UTF-8"?>
[62]<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:md="http://www.medico.com/schemas/record"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
[63]        access_control-xacml-2.0-policy-schema-os.xsd" PolicyId="http://authz-
interop.org/xacml/example/example822/policy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
[64] <Description>
[65]   Example 822 - Policy: Request: Simple Request-Policy-Response
[66]   </Description>
[67] <PolicyDefaults>
[68] <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-19991116</XPathVersion>
[69] </PolicyDefaults>
[70] <Target>
[71] <Subjects>
[72] <Subject>
[73] <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[74] <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
[75]        gin.ggf.nl</AttributeValue>
[76] <SubjectAttributeDesignator
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="http://authz-interop.org/xacml/subject/vo"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[77] </SubjectMatch>
[78] </Subject>
[79] </Subjects>
[80] <Resources>
[81] <Resource>
[82] <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[83]  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#URI">http://authz-
interop.org/xacml/resource/resource-type/se
[84]     </AttributeValue>
[85] <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#URI"/>
[86] </ResourceMatch>
[87] </Resource>
[88] </Resources>
[89] </Target>
[90] <Rule RuleId="http://authz-interop.org/xacml/example/example822/policy/rule01"
Effect="Permit">
[91]  <Description>
[92]        User with role "/gin.ggf.nl/APAC/Role=Researcher"  from "gin.ggf.nl" can execute action "http://authz-
interop.org/xacml/action/action-type/access" on the Resource "http://authz-interop.org/xacml/resource/resource-
type/se" from Target
[93]     </Description>
[94] <Target>
[95] <Actions>
[96] <Action>
[97] <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[98] <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">http://authz-
interop.org/xacml/action/action-type/access</AttributeValue>
```

```
[99] <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[100]      </ActionMatch>
[101]      </Action>
[102]      </Actions>
[103]      </Target>
[104]      <Condition>
[105]      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
[106]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/gin.ggf.nl/APAC/Role=VO-
Admin</AttributeValue>
[107]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/gin.ggf.nl/APAC/Role=Researcher</At
tributeValue>
[108]      <SubjectAttributeDesignator AttributeId="http://authz-
interop.org/xacml/subject/voms-primary-fqan"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[109]           </Apply>
[110]         </Condition>
[111]       </Rule>
[112]       <Obligations>
[113]         <Obligation ObligationId="http://authz-
interop.org/xacml/obligation/uidgid" FulfillOn="Permit">
[114]      <AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-uid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2501</AttributeAssignment>
[115]      <AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-gid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2101</AttributeAssignment>
[116]         </Obligation>
[117]       </Obligations>
[118] </Policy>
```

8.2. A.2 Example of Request/Response and Policy with simple negotiation between PEP and PDP about supported Obligations

This example demonstrates simple negotiation procedure between PEP and PDP about supported Obligations. For this purpose the PEP sends a Request message that contains the list of supported Obligations in the Environment element.

a) Request message that contains information about supporting Obligations in lines [163-178]

```
[119]      <?xml version="1.0" encoding="UTF-8"?>
[120]      <Request
[121]           xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
[122]           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[123]           xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
[124]             access_control-xacml-2.0-context-schema-os.xsd">
```

```
[125]        <!-- Example - Request: Supported Obligations negotiation - List of
supported by PEP Obligations are communicated as the Environment Attribute -->
[126]        <Subject>
[127]          <Attribute
[128]                AttributeId="http://authz-interop.org/xacml/subject/subject-
x509-id"
[129]                DataType="http://www.w3.org/2001/XMLSchema#string">
[130]             <AttributeValue>/O=dutchgrid/O=users/O=nikhef/CN=Wim
Huizinga</AttributeValue>
[131]          </Attribute>
[132]          <Attribute
[133]                AttributeId="http://authz-interop.org/xacml/subject/subject-
x509-issuer"
[134]                DataType="http://www.w3.org/2001/XMLSchema#string">
[135]             <AttributeValue>/C=NL/O=NIKHEF/CN=NIKHEF medium-security
certification auth</AttributeValue>
[136]          </Attribute>
[137]          <Attribute
[138]                AttributeId="http://authz-interop.org/xacml/subject/vo"
[139]                DataType="http://www.w3.org/2001/XMLSchema#string">
[140]            <AttributeValue>gin.ggf.nl</AttributeValue>
[141]          </Attribute>
[142]          <Attribute
[143]                AttributeId="http://authz-interop.org/xacml/subject/voms-
primary-fqan"
[144]                DataType="http://www.w3.org/2001/XMLSchema#string">
[145]            <AttributeValue>/gin.ggf.nl/APAC/Role=VO-Admin</AttributeValue>
[146]          </Attribute>
[147]        </Subject>
[148]        <Resource>
[149]          <Attribute
[150]               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
[151]               DataType="http://www.w3.org/2001/XMLSchema#anyURI">
[152]             <AttributeValue>http://authz-interop.org/xacml/resource/resource-
type/ce</AttributeValue>
[153]          </Attribute>
[154]        </Resource>
[155]        <Action>
[156]          <Attribute
[157]               AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[158]               DataType="http://www.w3.org/2001/XMLSchema#string">
[159]             <AttributeValue>http://authz-interop.org/xacml/action/action-
type/execute-now</AttributeValue>
[160]          </Attribute>
[161]        </Action>
[162]        <Environment>
[163]            <Attribute
[164]               AttributeId="http://authz-interop.org/xacml/environment/pep-
oblig-supported"
[165]               DataType="http://www.w3.org/2001/XMLSchema#string">
```

```
[166]            <AttributeValue>"http://authz-
interop.org/xacml/obligation/uidgid</AttributeValue>
[167]          </Attribute>
[168]            <Attribute
[169]               AttributeId="http://authz-interop.org/xacml/environment/pep-
oblig-supported"
[170]               DataType="http://www.w3.org/2001/XMLSchema#string">
[171]            <AttributeValue>http://authz-interop.org/xacml/obligation/secondary-
gids</AttributeValue>
[172]          </Attribute>
[173]            <Attribute
[174]               AttributeId="http://authz-interop.org/xacml/environment/pep-
oblig-supported"
[175]               DataType="http://www.w3.org/2001/XMLSchema#string">
[176]            <AttributeValue>http://authz-
interop.org/xacml/obligation/username</AttributeValue>
[177]          </Attribute>
[178]        </Environment>
[179]      </Request>
```

b) Response message with returned obligations in lines [188-193] to map user identity to returned UID and GID under which the user task/request will be executed.

```
[180]      <?xml version="1.0" encoding="UTF-8"?>
[181]      <Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[182]      xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
access_control-xacml-2.0-context-schema-os.xsd">
[183]        <Result ResourceId=" http://authz-interop.org/xacml/resource/resource-
type/ce">
[184]          <Decision>Permit</Decision>
[185]          <Status>
[186]      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
[187]          </Status>
[188]          <xacml:Obligations>
[189]      <xacml:Obligation ObligationId="http://authz-
interop.org/xacml/obligation/uidgid" FulfillOn="Permit">
[190]      <xacml:AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-uid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2501</xacml:AttributeAssignment>
[191]      <xacml:AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-gid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2001</xacml:AttributeAssignment>
[192]      </xacml:Obligation>
[193]        </xacml:Obligations>
[194]        </Result>
[195]      </Response>
```

c) Example policy that checks the list of supported Obligations using matching conditions in the Policy Target Environment in lines [226-235]. If the pep-oblig-supported attribute in the request does not contain the username or uidgid obligations, this policy evaluates to “Not applicable”.

```
[196]      <?xml version="1.0" encoding="UTF-8"?>
[197]      <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:md="http://www.medico.com/schemas/record"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
[198]              access_control-xacml-2.0-policy-schema-os.xsd"
PolicyId="http://authz-interop.org/xacml/example/example852/policy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
[199]      <Description>
[200]        Example 852 - Policy: Supported obligations negotiation - Sending list
of supported obligations as multiple Environment attributes.
[201]        In a simple case Policy Target must match all supported Obligations
[202]        </Description>
[203]      <PolicyDefaults>
[204]      <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-19991116</XPathVersion>
[205]      </PolicyDefaults>
[206]      <Target>
[207]      <Subjects>
[208]      <Subject>
[209]      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
[210]      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
[211]              gin.ggf.nl</AttributeValue>
[212]      <SubjectAttributeDesignator
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="http://authz-interop.org/xacml/subject/vo"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[213]      </SubjectMatch>
[214]      </Subject>
[215]      </Subjects>
[216]      <Resources>
[217]      <Resource>
[218]      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
[219]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#URI">http://authz-
interop.org/xacml/resource/resource-type/ce
[220]              </AttributeValue>
[221]      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#URI"/>
[222]      </ResourceMatch>
[223]      </Resource>
[224]      </Resources>
[225]      <Environments>
[226]      <Environment>
[227]      <EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
```

```
[228]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">http://authz-
interop.org/xacml/obligation/uidgid</AttributeValue>
[229]      <EnvironmentAttributeDesignator AttributeId="http://authz-
interop.org/xacml/environment/pep-oblig-supported"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[230]      </EnvironmentMatch>
[231]      <EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
[232]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">http://authz-
interop.org/xacml/obligation/username</AttributeValue>
[233]      <EnvironmentAttributeDesignator AttributeId="http://authz-
interop.org/xacml/environment/pep-oblig-supported"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[234]      </EnvironmentMatch>
[235]      </Environment>
[236]      </Environments>
[237]      </Target>
[238]      <Rule RuleId="http://authz-
interop.org/xacml/example/example852/policy/rule01" Effect="Permit">
[239]      <Description>
[240]             User with role "/gin.ggf.nl/APAC/Role=VO-Admin"  from "gin.ggf.nl"
can execute action "http://authz-interop.org/xacml/action/action-type/execute-now" on
the Resource "http://authz-interop.org/xacml/resource/resource-type/ce" from Target
[241]           </Description>
[242]      <Target>
[243]      <Actions>
[244]      <Action>
[245]      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[246]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">http://authz-
interop.org/xacml/action/action-type/execute-now</AttributeValue>
[247]      <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[248]      </ActionMatch>
[249]      </Action>
[250]      </Actions>
[251]      </Target>
[252]      <Condition>
[253]      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
[254]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/gin.ggf.nl/APAC/Role=VO-
Admin</AttributeValue>
[255]      <SubjectAttributeDesignator AttributeId="http://authz-
interop.org/xacml/subject/voms-primary-fqan"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[256]      </Apply>
[257]      </Condition>
[258]      </Rule>
[259]      <Obligations>
```

```
[260]      <Obligation ObligationId="http://authz-
interop.org/xacml/obligation/UIDGID" FulfillOn="Permit">
[261]      <AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-uid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2501</AttributeAssignment>
[262]      <AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-gid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2001</AttributeAssignment>
[263]      </Obligation>
[264]      </Obligations>
[265]      </Policy>
```

8.3. A.3 Example of Request/Response and Policy for Pilot Job submitting to Worker Node

a) Request message that contains information about the Pilot Job submitter in the Environment element in lines [291-302]

```
[266]      <?xml version="1.0" encoding="UTF-8"?>
[267]      <Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
[268]              access_control-xacml-2.0-context-schema-os.xsd">
[269]          <!-- Example - Request: Requesting decision from WN when submitting
user job from the Pilot Job - (full) information about the PJ submitter Subject is
included in the Environment attribute -->
[270]          <Subject>
[271]              <Attribute AttributeId="http://authz-
interop.org/xacml/subject/subject-x509-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
[272]                  <AttributeValue>/O=dutchgrid/O=users/O=nikhef/CN=Wim
Huizinga</AttributeValue>
[273]              </Attribute>
[274]              <Attribute AttributeId="http://authz-interop.org/xacml/subject/vo"
DataType="http://www.w3.org/2001/XMLSchema#string">
[275]                  <AttributeValue>gin.ggf.nl</AttributeValue>
[276]              </Attribute>
[277]              <Attribute AttributeId="http://authz-
interop.org/xacml/subject/voms-primary-fqan"
DataType="http://www.w3.org/2001/XMLSchema#string">
[278]
<AttributeValue>/gin.ggf.nl/APAC/Role=Researcher</AttributeValue>
[279]              </Attribute>
[280]          </Subject>
[281]          <Resource>
[282]              <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
[283]                  <AttributeValue>http://authz-
interop.org/xacml/resource/resource-type/wn</AttributeValue>
[284]              </Attribute>
[285]          </Resource>
```

```
[286]          <Action>
[287]              <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
[288]                  <AttributeValue>http://authz-interop.org/xacml/action/action-
type/execute-now</AttributeValue>
[289]              </Attribute>
[290]          </Action>
[291]          <Environment>
[292]              <!-- Here Subject attributes of the Pilot Job submitter are
included  -->
[293]              <Attribute AttributeId="http://authz-
interop.org/xacml/environment/pilot-job/subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
[294]                  <AttributeValue>/O=dutchgrid/O=users/O=nikhef/CN=Joop van der
Hoek</AttributeValue>
[295]              </Attribute>
[296]              <Attribute AttributeId="http://authz-
interop.org/xacml/environment/pilot-job/vo"
DataType="http://www.w3.org/2001/XMLSchema#string">
[297]                  <AttributeValue>gin.ggf.nl</AttributeValue>
[298]              </Attribute>
[299]              <Attribute AttributeId="http://authz-
interop.org/xacml/environment/voms-primary-fqan"
DataType="http://www.w3.org/2001/XMLSchema#string">
[300]                  <AttributeValue>/gin.ggf.nl/APAC/Role=VO-services-
manager</AttributeValue>
[301]              </Attribute>
[302]          </Environment>
[303]      </Request>
```

b) Response message with returned obligations in lines [318-323] to map user identity to returned UID and GID under which the user task/request will be executed.

```
[304]      <?xml version="1.0" encoding="UTF-8"?>
[305]      <Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[306]      xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
access_control-xacml-2.0-context-schema-os.xsd">
[307]        <Result ResourceId="http://authz-interop.org/xacml/resource/resource-
type/ce">
[308]          <Decision>Permit</Decision>
[309]          <Status>
[310]      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
[311]          </Status>
[312]          <xacml:Obligations>
[313]      <xacml:Obligation ObligationId="http://authz-
interop.org/xacml/obligation/uidgid" FulfillOn="Permit">
[314]      <xacml:AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-uid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2501</xacml:AttributeAssignment>
```

```
[315]      <xacml:AttributeAssignment AttributeId="http://authz-
interop.org/xacml/attribute/posix-gid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2001</xacml:AttributeAssignment>
[316]      </xacml:Obligation>
[317]        </xacml:Obligations>
[318]        </Result>
[319]      </Response>
```

c) Example policy allows matching between pilot request/owner VO and pilot job submitter VO.

- Policy contains two rules: rule001 in lines [364-374] that checks user attribute, and rule002 in lines [375-391] that compares pilot request/owner VO and pilot job submitter VO
- AttributeSelect in the Apply element uses XPath expression in lines [386] to obtain submitters VO information from the Environment element in the Request

```
[320]      <?xml version="1.0" encoding="UTF-8"?>
[321] <Policy
[322]     xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[323]     xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
[324]     xmlns:md="http://www.medico.com/schemas/record"
[325]     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[326]     xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
[327]       access_control-xacml-2.0-policy-schema-os.xsd"
[328]     PolicyId="http://authz-interop.org/xacml/example/policy/example832/policy"
[329]     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
[330]  <Description>
[331]            Example - Policy Pilot job submission at WN: When submitting the User/real job the User VO
must match the Pilot Job submitter VO provided in the Environment element.
[332] </Description>
[333]  <PolicyDefaults>
[334]    <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-19991116</XPathVersion>
[335]  </PolicyDefaults>
[336]  <Target>
[337]    <Subjects>
[338]      <Subject>
[339]        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[340]        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">gin.ggf.nl</AttributeValue>
[341]        <SubjectAttributeDesignator SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"
[342]        AttributeId="http://authz-interop.org/xacml/subject/vo"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[343]        </SubjectMatch>
[344]      </Subject>
[345]    </Subjects>
[346]    <Resources>
[347]      <Resource>
[348]        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
[349]       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">http://authz-
interop.org/xacml/resource/resource-type/wn
[350]       </AttributeValue>
[351]         <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#URI"/>
[352]      </ResourceMatch>
[353]     </Resource>
[354]   </Resources>
[355]     <Actions>
[356]       <Action>
[357]         <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[358]           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">http://authz-
interop.org/xacml/action/action-type/execute-now</AttributeValue>
[359]           <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[360]         </ActionMatch>
[361]       </Action>
[362]     </Actions>
[363]   </Target>
[364]   <Rule RuleId="http://authz-interop.org/xacml/example/policy/example832/rule001" Effect="Permit">
[365]     <Description>
[366]       Rule001: User with role "/gin.ggf.nl/APAC/Role=Researcher"  from "gin.ggf.nl" can execute action
"http://authz-interop.org/xacml/action/action-type/execute-now" on the Resource under condition of Rule002 [373]
</Description>
[367]     <Target/>
[368]     <Condition>
[369]       <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[370]         <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/gin.ggf.nl/APAC/Role=Researcher</AttributeValue>
[371]       <SubjectAttributeDesignator AttributeId="http://authz-interop.org/xacml/subject/voms-primary-fqan"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
[372]       </Apply>
[373]     </Condition>
[374]   </Rule>
[375]   <Rule RuleId="http://authz-interop.org/xacml/example/policy/example832/rule002" Effect="Permit">
[376]     <Description>
[377]         Rule002: Additional conditionthat the User "subject/vo" matches Pilot Job submitter "environment/vo".
[378]     </Description>
[379]     <Target/>
[380]     <Condition>
[381]       <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[382]         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
[383]           <SubjectAttributeDesignator AttributeId="http://authz-interop.org/xacml/subject/vo"
DataType="http://www.w3.org/2001/XMLSchema#string"/>   [391]             </Apply>
[384]         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
[385]           <AttributeSelector DataType="http://www.w3.org/2001/XMLSchema#string"
[386]           RequestContextPath="./xacml-context:Environment/xacml-context:Attribute(@AttributeId,
'http://authz-interop.org/xacml/environment/pilot-job/vo')/xacml-context:AttributeValue/text()"
```

```
[387]            />
[388]          </Apply>
[389]        </Apply>
[390]      </Condition>
[391]    </Rule>
[392]    <Obligations>
[393]      <Obligation ObligationId="http://authz-interop.org/xacml/obligation/uidgid" FulfillOn="Permit">
[394]        <AttributeAssignment AttributeId="http://authz-interop.org/xacml/attribute/posix-uid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2501</AttributeAssignment>
[395]        <AttributeAssignment AttributeId="http://authz-interop.org/xacml/attribute/posix-gid"
DataType="http://www.w3.org/2001/XMLSchema#integer">2101</AttributeAssignment>
[396]      </Obligation>
[397]        </Obligations>
[398]      </Policy>
```

9. Appendix B: List of Attribute and Obligation IDs introduced by this profile

9.1. Subject Context

http://authz-interop.org/xacml/subject/subject-x509-id
http://authz-interop.org/xacml/subject/subject-condor-canonical-name-id
http://authz-interop.org/xacml/subject/subject-x509-issuer
http://authz-interop.org/xacml/subject/vo
http://authz-interop.org/xacml/subject/voms-signing-subject
http://authz-interop.org/xacml/subject/voms-signing-issuer
http://authz-interop.org/xacml/subject/voms-fqan
http://authz-interop.org/xacml/subject/voms-primary-fqan
http://authz-interop.org/xacml/subject/certificate-serial-number
http://authz-interop.org/xacml/subject/validity-not-before
http://authz-interop.org/xacml/subject/validity-not-after

9.2. Optional Subject Context:

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

9.3. Action Context

Enumeration of possible values for urn:oasis:names:tc:xacml:1.0:action:action-id :
http://authz-interop.org/xacml/action/action-type/queue
http://authz-interop.org/xacml/action/action-type/execute-now
http://authz-interop.org/xacml/action/action-type/access
http://authz-interop.org/xacml/action/rsl-string

9.4. Resource Context

Enumeration of possible values for urn:oasis:names:tc:xacml:1.0:resource:resource-id :
http://authz-interop.org/xacml/resource/resource-type/ce
http://authz-interop.org/xacml/resource/resource-type/se

http://authz-interop.org/xacml/resource/resource-type/wn
http://authz-interop.org/xacml/resource/dns-host-name
http://authz-interop.org/xacml/resource/resource-x509-id
http://authz-interop.org/xacml/resource/resource-x509-issuer

9.5. Environment Context

http://authz-interop.org/xacml/environment/pep-oblig-supported
http://authz-interop.org/xacml/environment/pilot-job/subject-x509-id
http://authz-interop.org/xacml/environment/pilot-job/subject-condor-canonical-name-id
http://authz-interop.org/xacml/environment/pilot-job/subject-x509-issuer
http://authz-interop.org/xacml/environment/pilot-job/vo
http://authz-interop.org/xacml/environment/pilot-job/voms-signing-subject
http://authz-interop.org/xacml/environment/pilot-job/voms-signing-issuer
http://authz-interop.org/xacml/environment/pilot-job/voms-fqan
http://authz-interop.org/xacml/environment/pilot-job/voms-primary-fqan

9.6. Obligation Context and Attributes

http://authz-interop.org/xacml/obligation/uidgid
http://authz-interop.org/xacml/attribute/posix-uid
http://authz-interop.org/xacml/attribute/posix-uid

http://authz-interop.org/xacml/obligation/secondary-gids
http://authz-interop.org/xacml/attribute/posix-gid

http://authz-interop.org/xacml/obligation/username
http://authz-interop.org/xacml/attribute/username

http://authz-interop.org/xacml/obligation/root-and-home-paths
http://authz-interop.org/xacml/attribute/rootpath
http://authz-interop.org/xacml/attribute/homepath

http://authz-interop.org/xacml/obligation/storage-access-priority
http://authz-interop.org/xacml/attribute/storage-priority

http://authz-interop.org/xacml/obligation/access-permissions
http://authz-interop.org/xacml/attribute/access-permissions

10. Document Change Log

V1.2i: Integrated several rounds of feedback feedback from OGF reviewers
v1.2b: Reformatting following the OGF template. Added Security considerations. March 9, 2012
v1.2: Added attributes for credential validity time; made certificate-serial-number non-optional; updated author list. Aug 5, 2011
v1.1: Fixed minor namespace inconsistencies in v1.0. Oct 09, 2008
v1.0: First release of the standard. May 16, 2008

11. Contributors

The authors of this document would like to acknowledge the contributions of the following people that have made this document possible over the past years in its developments.

Ian Alderman 9
Mine Altunay 1
Rachana Ananthakrishnan 8
Joe Bester 8
Keith Chadwick 1
Vincenzo Ciaschini 7
Yuri Demchenko 4
Andrea Ferraro 7
Alberto Forti 7
Gabriele Garzoglio 1
David Groep 2
Ted Hesselroth 1
John Hover 3
Oscar Koeroo 2
Chad La Joie 5
Tanya Levshina 1
Zach Miller 9
Jay Packard 3
Håkon Sagehaug 6
Valery Sergeev 1
Igor Sfiligoi 1
Neha Sharma 1
Frank Siebenlist 8
Valerio Venturi 7
John Weigand 1

1 Fermilab, Batavia, IL, USA
2 NIKHEF, Amsterdam, The Netherlands
3 Brookhaven National Laboratory, Upton, NY, USA
4 University of Amsterdam, Amsterdam, The Netherlands
5 SWITCH, Zürich, Switzerland
6 BCCS, Bergen, Norway
7 INFN CNAF, Bologna, Italy
8 Argonne National Laboratory, Argonne, IL, USA
9 University of Wisconsin, Madison, WI, USA

The editors and main authors of the document are:

Rachana Ananthakrishnan
Argonne National Laboratory
9700 South Cass Avenue
Building 240
Argonne, IL 60439-4844
Email: ranantha@mcs.anl.gov

Gabriele Garzoglio
Fermilab
P.O. Box 500
Batavia, IL 60510-5011
United States of America

Email: garzogli@fnal.gov

Oscar Koeroo
Postbus 41882
1009 DB, Amsterdam
The Netherlands
Email: okoeroo@nikhef.nl

12. Acknowledgments

This work was supported in part by the Office of Advanced Scientific Computing Research, Office of Science, U.S. Dept. of Energy, under Contract DE-AC02-06CH11357.

Fermilab is operated by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the United States Department of Energy. This work was partially funded by the Office of Advanced Scientific Computing Research, Office of Science, U.S. Dept. of Energy, under Contract DE-AC02-06CH11357.

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

We thank the people who commented on this profile, in particular David Chadwick, Paul Millar, and Jules Wolfrat. A special thank to Alan Sill and Jens Jensen for their help throughout the standardization process.

13. 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.

14. 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.

15. Full Copyright Notice

16. References

[GUMS] Lorch M, Kafura D, Fisk I, Keahey K, Carcassi G, Freeman T, Peremutov T, Rana AS. 2005. Authorization and account management in the Open Science Grid *Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing*, 2005

[SCAS] Groep D. 2008. gLExec, SCAS and the way forward *Proceedings of the EGEE08 Conference - the Middleware Security Group, Istanbul, Turkey*

[SAZ] Chadwick K, Sharma N, Timm SC, Yocum DR. 2009. FermiGrid – Site AuthoriZation (SAZ) Service *Proceedings of Computing in High Energy Physics and Nuclear Physics 2009, Prague, Czech Republic*

[BRADNER] “RFC 2119: Key words for use in RFCs to Indicate Requirement Levels”

[XACML] “eXtensible Access Control Markup Language (XACML) Version 2.0”
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[XMLSchema] “XML Schema Part 2: Datatype 2nd Edition”:
http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/

[HTCondor] Douglas Thain, Todd Tannenbaum, and Miron Livny, "Distributed Computing in Practice: The Condor Experience" *Concurrency and Computation: Practice and Experience*, Vol. 17, No. 2-4, pages 323-356, February-April, 2005.

[FQAN] V. Ciaschini, V. Venturi, A. Ceccanti, “The VOMS attribute Certificate Format”, GFD-I.182, Aug 2011

[RSL] “GT 2.4: The Globus Resource Specification Language RSL v1.0”
http://www.globus.org/toolkit/docs/2.4/gram/rsl_spec1.html