GFD-I.182
Category – Informational
OGSA Authorization working group

Vincenzo Ciaschini, INFN CNAF
Valerio Venturi, INFN CNAF
Andrea Ceccanti, INFN CNAF

August 1, 2011

The VOMS Attribute Certificate Format

Status of This Memo

This document provides a description of the VOMS AC. Distribution is unlimited.

Copyright Notice

Abstract

This document provides a complete description of the VOMS AC format, both syntax and semantics. It also describes the related extensions that must be used in a proxy certificate to make it fully VOMS-compliant.

Contents

1. Introduction

This document is a companion to the “Attributes used in OGSA Authorization” GWD 57 [OGSI-Authz-Attrs] and also requires knowledge of RFC 5755, RFC 5280, RFC 3820, though to simplify understanding part of the information from those documents will be duplicated here.

Attribute Certificates (ACs) provide a standardized method to associate a set of attributes to an identity. However, they may be created in thousand of different ways and so it becomes necessary to also have a complete description of the expected format of the AC before it can be used in an application.

The aim of this document is to provide a complete specification of the Attribute Certificates generated by VOMS, to simplify and ensure interoperability among services that need to parse and interpret them.

Section 2 will give a very brief account of conventions and abbreviations used in this specification; Section 3 will document the format of the AC; section 4 will document how ACs are included in a proxy certificate. Section 5 will present a (non-normative) example of a proxy containing a VOMS attribute certificate. Finally, section 6 will briefly talk about security considerations.

2. Conventions used in this Specification

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

The following abbreviations will also be used: AC (Attribute Certificate), AA (Attribute Authority), PKC (Public Key Certificate), FQHN (Fully Qualified Host Name), FQAN (Fully Qualified Attribute Name).

3. AC Format

This is the general format of an AC as defined by RFC 5755. Customizations used by VOMS will be discussed in individual subsections. Everything not specifically mentioned here is intended to be in accordance with RFC 5755.

```
AttributeCertificate ::= SEQUENCE {
  acinfo              AttributeCertificateInfo,
  signatureAlgorithm  AlgorithmIdentifier,
  signatureValue      BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
  version                AttCertVersion,
  holder                 Holder,
  issuer                 AttCertIssuer,
  signature              AlgorithmIdentifier,
  serialNumber           CertificateSerialNumber,
  attrCertValidityPeriod AttCertValidityPeriod,
  attributes             SEQUENCE OF Attribute,
  issuerUniqueID         UniqueIdentifier OPTIONAL,
  extensions             Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v2(1) }

Holder ::= SEQUENCE {
  baseCertificateID   [0] IssuerSerial OPTIONAL,
  entityName          [1] GeneralNames OPTIONAL,
  objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
}
```

```
AttCertIssuer ::= CHOICE {
  v2Form   [0] V2Form
}

V2Form ::= SEQUENCE {
  issuerName            GeneralNames  OPTIONAL,
  baseCertificateID     [0] IssuerSerial  OPTIONAL,
  objectDigestInfo      [1] ObjectDigestInfo  OPTIONAL
}

IssuerSerial  ::=  SEQUENCE {
  issuer         GeneralNames,
  serial         CertificateSerialNumber,
  issuerUID      UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod  ::= SEQUENCE {
  notBeforeTime  GeneralizedTime,
  notAfterTime   GeneralizedTime
}

Attribute ::= SEQUENCE {
  type      AttributeType,
  values    SET OF AttributeValue
  -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

Also, the `voms` OID is defined and reserved for VOMS uses, and its value is 1.3.6.1.4.1.8005.100.100

3.1 Holder

3.1.1 Syntax

The holder of a VOMS AC MUST always be an X.509 PKC. As a consequence of this, in VOMS ACs the only admissible choice for the field is the `baseCertificateID`, while `entityName` and `objectDigestInfo` MUST be absent. This means that the `IssuerSerial` structure MUST be used for this field.

3.1.2 Semantics

The `issuer` and `serial` fields MUST be copies of those in the holder's PKC, while the `issuerUID` field is usually empty. It MUST be present if and only if it is also present in the holder's PKC, where it is named `subjectUniqueID`, and in this case they MUST have the same value. Note that RFC 5280 says that conforming implementations CAs MUST NOT generate certificates which include this field, but that implementations SHOULD be capable of parsing it.

Note that the holder here is the user's own PKC, and NOT the proxies he may use.

3.2 AttCertIssuer

3.2.1 Syntax

RFC 5755 requires that the `V2Form` MUST be used to specify the `AttCertIssuer` field. Furthermore, it requires that only the `issuerName` field be used and that it MUST contain just one `GeneralName`, which in turn must contain only a single distinguished name in its `directoryName` field.

3.2.2 Semantics

The included distinguished name MUST be the distinguished name of the issuer's own PKC. This in turn requires that the issuer's PKC MUST have a non-empty distinguished name, as required by RFC 5755.

3.3 AttCertValidityPeriod

3.3.1 Syntax & Semantics

This is a standard validity field. It defines the times of start and end validity for the whole AC. Its values should be expressed in the UTC timezone, with seconds always included.

3.4 Attribute

This is the core of the AC, where the important data actually is. The following subsections will describe the attributes that are used by VOMS. Further attributes than those defined here MAY be present and, if so, conforming application MAY choose to ignore them.

The attributes `Role` and `Group` defined in RFC 5755 SHOULD NOT be used. Instead a new attribute, `FQAN` (see below) is defined.

3.4.1 Attribute Fully Qualified Attribute Name (FQAN)

3.4.1.1 Syntax

This attribute uses the following syntax:

```
name          : voms-attribute
OID           : { voms 4 }
syntax        : IetfAttrSyntax
values        : Multiple not allowed
```

`IetfAttrSyntax` is defined in RFC 5755 and reprinted here for convenience:

```
IetfAttrSyntax ::= SEQUENCE {
  policyAuthority [0] GeneralNames    OPTIONAL,
  values SEQUENCE OF CHOICE {
    octets    OCTET STRING,
    oid       OBJECT IDENTIFIER,
    string    UTF8String
  }
}
```

The `policyAuthority` field of the `IetfAttrSyntax` MUST be present and MUST contain an encoding of both the VO to which the AC issuer belongs and the server which generated this particular attribute, in the following format: `<vo name>://<fqhn>:<port>`, where the characters '<' and '>' are only used to highlight the field names and should not be used in the actual encoding.

This attribute MUST be present in a conforming AC. If multiple values are needed (and usually they are), they can be encoded in the `values` SEQUENCE. The `octets` encoding of `values` MUST be used.

3.4.1.2 Semantics

This attribute encodes the position of the Holder inside the VO. A Holder may be a member of several groups, and he may hold a special role inside some of his groups.

Groups are organized in a tree structure, meaning that a group may have subgroups, which in turn may have subgroups, etc… The group name is then represented in the following way:

```
/<root group>/<subgroup>/…/<subgroup>
```

Where <root group> MUST be the name of the virtual organization.

The hierarchical structure implies that if someone is a member of a subgroup, than he is also member of the parent group. For example, membership of:

```
/<root group>/<subgroup>
```

implies membership in:

```
/<root group>
```

And thus both FQANs will be present in the AC.

Roles are not organized in a hierarchical structure. Ownership of a role is always associated to membership in a group. Ownership of a role in a specific subgroup does not say anything about ownership of that role in the parent group. It is consequently possible to hold role X in a subgroup, but not in its parent group.

All groups of which the Holder is a member are represented in the attribute, but no information on role ownership is represented unless the Holder specifically asked for it while contacting the Attribute Authority (AA). This is indeed the main difference between groups and roles: group membership is compulsory and cannot be denied, while role ownership is an optional thing that the holder may or may not want to be specified.

This information is encoded in a Fully Qualified Attribute Name (FQAN), in the following format:

```
<group name>/Role=<role name>/Capability=<capability name>
```

This syntax means that the user holds the role `<role name>` in the group `<group name>`. If no specific role is held, the `<role name>` is `NULL`. The `/Capability=<capability name>` part is deprecated and will disappear in the future: conforming applications SHOULD be able to handle FQANs where it is absent and SHOULD NOT rely on its presence. New applications MUST be able to handle FQANs where it is absent, and MUST NOT rely on its presence.

Compatibility issue: a `/Role=NULL` component may be omitted in its entirety. The same goes for a `/Capability=NULL` part. Conforming applications SHOULD be prepared to handle these cases. New application MUST be able to handle the absence of these components.

The order in which the FQANs are present in the attribute is significant, since it is the order in which the Holder wished the FQANs to be evaluated. Conforming applications SHOULD be capable of accepting an unlimited number of FQANs, however if an application is not capable of this but is limited to accept only `n`, then they MUST be the first `n` present in this extension. In particular, if an application can accept only one FQAN, then it MUST be the first one. Conforming applications MUST respect the order in which the FQANs are present in the AC and MUST evaluate them in that order.

3.4.1.3 Examples

Examples of valid FQANs:

```
/cms/Role=NULL/Capability=NULL

/cms/Role=VO-Admin/Capability=NULL
```

```
/cms/Role=sgm/Capability=NULL
/cms/production/Role=NULL/Capability=NULL
/cms/production/Role=writer/Capability=NULL
/cms/analysis/Role=NULL/Capability=NULL
/www.project.org/members/Role=NULL/Capability=NULL
```

The same FQANs in the compact format:

```
/cms
/cms/Role=VO-Admin
/cms/Role=sgm
/cms/production
/cms/production/Role=writer
/cms/analysis
/www.project.org/members
```

3.4.1.4 FQAN formal grammar

```
fqan::= groups
        |   groups  '/Role=' rolename

groups ::= '/' groupname
            |    groups '/' groupname

groupname ::= rolename
rolename ::= [a-zA-Z0-9][a-zA-Z0-9_.-]*
```

whitespace among the elements of the grammar is forbidden.

3.5 IssuerUniqueID

This field should be present if and only if it is also present in the issuer's certificate, in which case the two MUST be identical.

3.6 Extensions

Here will be defined the extensions that are defined for use into the VOMS AC. Other extensions may still be present, but they MUST NOT be critical.

3.6.1 ACTarget

3.6.1.1 Syntax

```
      name            id-ce-targetInformation
      OID             { id-ce 55 }
      syntax          SEQUENCE OF Targets
      criticality     MUST be TRUE

      Targets ::= SEQUENCE OF Target

      Target  ::= CHOICE {
         targetName          [0] GeneralName,
         targetGroup          [1] GeneralName,
         targetCert           [2] TargetCert
      }

      TargetCert  ::= SEQUENCE {
         targetCertificate    IssuerSerial,
         targetName           GeneralName OPTIONAL,
         certDigestInfo       ObjectDigestInfo OPTIONAL
      }
```

When this extension is used `targetName` MUST be the chosen encoding. It MUST contain the URI of a resource, encoded in the `IA5STRING` format.

If the `ACTarget` extension is present, conforming applications MUST honour it.

3.6.1.2 Semantics

The intent of the `ACTarget` extension is to be able to specify the exact set of targets where the AC can be accepted. If the AC is evaluated on any other resource than those listed in the extension, then the evaluation of the AC SHOULD fail. To this intent, the content of the extension is supposed to be a set of fully qualified domain names, indicating where verification of the AC can succeed. If the `ACTarget` extension is not present, than this test is always passed. An example of when evaluation should not fail is when the AC is read only for information purposes, for example to show the user its contents.

3.6.2 NoRevAvail

3.6.2.1 Syntax

```
      name           id-ce-noRevAvail
      OID            { id-ce 56 }
      syntax         NULL (i.e. '0500'H is the DER encoding)
      criticality    MUST be FALSE
```

3.6.2.2 Semantics

No Revocation Available. The intent of this extension is to specify that a CRL for the AA may not exist, and even should they exist they will NEVER refer to this AC.

3.6.3 IssuerCerts

3.6.3.1 Syntax

```
      name           pk-cert-list
      OID            { voms 10 }
      syntax         X509_CERTS
      criticality    MUST be FALSE
```

```
            X509_CERTS ::= SEQUENCE OF X509Certificate
```

3.6.3.2 Semantics

The `IssuerCerts` extension is meant to include the AA's public key certificate and the whole certificate chain leading to it, up to and excluding the CA certificate that is expected to be on the evaluator's machine (typically, the root CA).

Applications MAY use the certificate chain present in the `IssuerCerts` extension to evaluate the AC without requiring that the VOMS server certificate is distributed to the relying parties. However, blindly trusting it introduces a security issue because than anyone could sign a certificate for every VO. To avoid this, relying applications MUST have a local method to know that the included certificate chain actually identifies a trusted AA.

For example, one such method may be to know in advance the subject and issuer of the certificates comprising the chain, and confronting this locally known description with what is present in the extension, and fail the evaluation if they do not match.

3.6.4 Tags

3.6.4.1 Syntax

```
name          : tags
OID           : { voms 11 }
syntax        : TagContainer
values        : Multiple not allowed
```

```
TagContainer ::= SEQUENCE OF TagList
TagList ::= SEQUENCE {
         policyAuthority GeneralNames,
         tags SEQUENCE OF Tag
       }
       Tag ::= SEQUENCE {
         name      OCTET STRING
         value     OCTET STRING
         qualifier OCTET STRING
       }
```

The `policyAuthority` field follows the `IetfAttrSyntax.policyAuthority` (defined above in 3.4.1.1) syntax and, if both attributes are present, they MUST be set to the same sequence.

3.6.4.2 Semantics

The intent of this extension is to provide a way to specify attributes that do not map well in the group/role paradigm. It allows for this by specifying a set of (name, value, qualifier) triples that could be used to describe almost everything.

Not all conforming applications need to understand the semantics associated to each `Tag` name. In such a case the tags MAY be safely ignored.

If multiple `value`s need to be associated with a single `name`, it is possible to use several (`name, value, qualifier`) `Tag`s with the same name, and possibly different qualifiers. A name-specific syntax that encodes multiple values in a single `Tag` is also allowed. Conforming applications that are aware of a specific `name` MUST consider the two syntaxes as completely equivalent. The same `Tag` MUST NOT appear more than once.

The `policyAuthority` is specific to each `TagList` object, and MUST indicate the name of the authority that is the source of the enclosed tags. This is generally the VOMS server which issued the AC. However, in case the tags have been synchronized from an external source, it MAY be the name of hat source.

4. VOMS compliant proxy certificates

ACs, once created, need to become available to applications that want to use the information they contain. To both maintain the single login feature of the grid, and to let the user choose what ACs to present to an application, the best way is to include them in the user's proxy certificate. The intent of this section is to show how this is done.

The following defines how VOMS Attribute Certificates are to be attached as extensions to Proxy certificates. Other extensions than those listed may be included in the proxy itself but are out of scope of this document. Note that including critical extensions may result in the proxy becoming unreadable, and

4.1 AC Sequence

4.1.1 Syntax

```
name: acseq
OID: { voms 5 }
Syntax: acSequence

acSequence = SEQUENCE OF AttributeCertificate
```

4.1.2 Semantics

This is the way to include ACs generated by VOMS inside a certificate. They should be included in the order in which they were requested. Conforming applications that are not capable of accepting multiple ACs SHOULD at least accept the first, the "Default" VO.

4.2 KeyUsage extension

This extension MUST always be present. Its values SHOULD at least include the `digitalSignature`, `keyEncipherment` and `dataEncipherment` bits.

4.3 Obsolete Extensions

Due to compatibility with old, pre-AC version of VOMS, it is possible to find in VOMS proxies extensions with OID 1.3.6.1.4.1.8005.100.100.6 and 1.3.6.1.4.1.8005.100.100.1. These are obsolete now and can be safely ignored. For this reason, their syntax and semantics is not documented.

4.4 Proxy certificate chain handling

During normal job execution in a grid environment, a proxy may be delegated several times, and each delegated proxy may obtain a new set of AC. This subsection will detail how these ACs MUST be evaluated.

Let us call the user certificate $cert_0$. The proxy generated from it is $cert_1$, the proxy generated from $cert_1$ is $cert_2$, and so on until the latest delegation, called $cert_N$.

During the evaluation procedure, the chain is parsed in order from $cert_N$ to $cert_0$. When an AC is found in $cert_I$, all subsequent ACs in $cert_J$ with $J<I$ MUST be ignored. In other words, only the most recent attribute certificate must be evaluated.

5. Non-normative example

This section will present an example of a proxy certificate containing an AC issued by VOMS. This is an RFC 3820-compliant proxy, including VOMS extensions. Please note that line starting with '#' are comments, and not part of the actual structure.

```
# Certificate starts
   0 1861: SEQUENCE {
   4 1710: . SEQUENCE {
   8    3: . . [0] {
  10    1: . . . INTEGER 2
         : . . . }
  13    1: . . INTEGER 1
  16   13: . . SEQUENCE {
  18    9: . . . OBJECT IDENTIFIER md5withRSAEncryption (1 2 840 113549 1 1 4)
  29    0: . . . NULL
         : . . . }
  31   27: . . SEQUENCE {
  33   11: . . . SET {
  35    9: . . . . SEQUENCE {
  37    3: . . . . . OBJECT IDENTIFIER countryName (2 5 4 6)
  42    2: . . . . . PrintableString 'IT'
         : . . . . . }
         : . . . . }
  46   12: . . . SET {
  48   10: . . . . SEQUENCE {
  50    3: . . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
  55    3: . . . . . PrintableString '001'
         : . . . . . }
         : . . . . }
         : . . . }
  60   30: . . SEQUENCE {
  62   13: . . . UTCTime 04/11/2010 15:42:03 GMT
  77   13: . . . UTCTime 05/11/2010 03:47:03 GMT
         : . . . }
  92   47: . . SEQUENCE {
  94   11: . . . SET {
  96    9: . . . . SEQUENCE {
  98    3: . . . . . OBJECT IDENTIFIER countryName (2 5 4 6)
 103    2: . . . . . PrintableString 'IT'
         : . . . . . }
         : . . . . }
 107   12: . . . SET {
 109   10: . . . . SEQUENCE {
 111    3: . . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
 116    3: . . . . . PrintableString '001'
         : . . . . . }
         : . . . . }
 121   18: . . . SET {
 123   16: . . . . SEQUENCE {
 125    3: . . . . . OBJECT IDENTIFIER commonName (2 5 4 3)
 130    9: . . . . . PrintableString '578100657'
         : . . . . . }
         : . . . . }
         : . . . }
 141  159: . . SEQUENCE {
 144   13: . . . SEQUENCE {
 146    9: . . . . OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
 157    0: . . . . NULL
         : . . . . }
 159  141: . . . BIT STRING, encapsulates {
 163  137: . . . . SEQUENCE {
 166  129: . . . . . INTEGER
         : . . . . . . 00 A1 43 03 19 02 D5 87 25 29 24 53 BB F3 DA A4
         : . . . . . . 85 87 41 B9 B5 BD C3 8C 59 D9 2B 0E EC 8C 41 EA
         : . . . . . . 9E 40 3E 61 6E EF 64 0E FD B6 59 E6 51 5D BA 4C
         : . . . . . . 10 87 5F 70 C7 41 AF C0 50 97 B4 E1 7B B1 B0 A2
         : . . . . . . 52 BF AD EB D3 E6 77 0D EE 1E 78 BE DF 04 7A 86
         : . . . . . . A9 23 07 5A DE D8 EE F5 7A A5 45 99 EA 74 4A C0
```

```
        : . . . . . . . B4 F8 6C 1D 6E 73 D2 92 6E 24 37 67 7B 93 D6 C1
        : . . . . . . . AB A2 D6 6F 00 44 EB 72 3B C7 54 97 77 93 BA 42
        : . . . . . . . . . . . [ Another 1 bytes skipped ]
 298    3: . . . . . INTEGER 65537
        : . . . . . }
        : . . . . }
        : . . . }
 303 1411: . . [3] {
 307 1407: . . . SEQUENCE {
 311 1338: . . . . SEQUENCE {
# The VOMS extension starts here
 315   10: . . . . . OBJECT IDENTIFIER '1 3 6 1 4 1 8005 100 100 5'
 327 1322: . . . . . OCTET STRING, encapsulates {
 331 1318: . . . . . . SEQUENCE {
 335 1314: . . . . . . . SEQUENCE {
 339 1310: . . . . . . . . SEQUENCE {
 343 1159: . . . . . . . . . SEQUENCE {
 347    1: . . . . . . . . . . INTEGER 1
 350   38: . . . . . . . . . . SEQUENCE {
 352   36: . . . . . . . . . . . [0] {
 354   31: . . . . . . . . . . . . SEQUENCE {
 356   29: . . . . . . . . . . . . . [4] {
 358   27: . . . . . . . . . . . . . . SEQUENCE {
 360   11: . . . . . . . . . . . . . . . SET {
 362    9: . . . . . . . . . . . . . . . . SEQUENCE {
 364    3: . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . countryName (2 5 4 6)
 369    2: . . . . . . . . . . . . . . . . . PrintableString 'IT'
        : . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . }
 373   12: . . . . . . . . . . . . . . . SET {
 375   10: . . . . . . . . . . . . . . . . SEQUENCE {
 377    3: . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . commonName (2 5 4 3)
 382    3: . . . . . . . . . . . . . . . . . PrintableString '001'
        : . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . }
 387    1: . . . . . . . . . . . . . INTEGER 1
        : . . . . . . . . . . . . . }
        : . . . . . . . . . . . . }
 390   33: . . . . . . . . . . . [0] {
 392   31: . . . . . . . . . . . . SEQUENCE {
 394   29: . . . . . . . . . . . . . [4] {
 396   27: . . . . . . . . . . . . . . SEQUENCE {
 398   11: . . . . . . . . . . . . . . . SET {
 400    9: . . . . . . . . . . . . . . . . SEQUENCE {
 402    3: . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . countryName (2 5 4 6)
 407    2: . . . . . . . . . . . . . . . . . PrintableString 'IT'
        : . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . }
 411   12: . . . . . . . . . . . . . . . SET {
 413   10: . . . . . . . . . . . . . . . . SEQUENCE {
 415    3: . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . commonName (2 5 4 3)
 420    3: . . . . . . . . . . . . . . . . . PrintableString '003'
        : . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . }
        : . . . . . . . . . . . . }
 425   13: . . . . . . . . . . . SEQUENCE {
 427    9: . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . md5withRSAEncryption (1 2 840 113549 1 1 4)
 438    0: . . . . . . . . . . . . NULL
        : . . . . . . . . . . . . }
 440   16: . . . . . . . . . . . INTEGER
```

```
         : . . . . . . . . . . 6E 62 B2 4B A7 7C 4F 48 BB 11 A7 66 53 1E D1 31
 458   34: . . . . . . . . . . . SEQUENCE {
 460   15: . . . . . . . . . . . . GeneralizedTime 04/11/2010 15:47:03 GMT
 477   15: . . . . . . . . . . . . GeneralizedTime 05/11/2010 03:47:03 GMT
         : . . . . . . . . . . . . }
# The voms-attribute extension (section 3.4.1)
 494   84: . . . . . . . . . . . SEQUENCE {
 496   82: . . . . . . . . . . . . SEQUENCE {
 498   10: . . . . . . . . . . . . . OBJECT IDENTIFIER '1 3 6 1 4 1 8005 100 100 4'
 510   68: . . . . . . . . . . . . . SET {
 512   66: . . . . . . . . . . . . . . SEQUENCE {
 514   39: . . . . . . . . . . . . . . . [0] {
 516   37: . . . . . . . . . . . . . . . . [6] 'voms1://testbed002.cnaf.infn.it:33334'
         : . . . . . . . . . . . . . . . . }
 555   23: . . . . . . . . . . . . . . . SEQUENCE {
 557    6: . . . . . . . . . . . . . . . . OCTET STRING '/voms1'
 565   13: . . . . . . . . . . . . . . . . OCTET STRING '/voms1/group1'
         : . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . }
         : . . . . . . . . . . . . }
# The tags extension (section 3.6.4)
 580  922: . . . . . . . . . . . SEQUENCE {
 584  127: . . . . . . . . . . . . SEQUENCE {
 586   10: . . . . . . . . . . . . . OBJECT IDENTIFIER '1 3 6 1 4 1 8005 100 100 11'
 598  113: . . . . . . . . . . . . . OCTET STRING, encapsulates {
 600  111: . . . . . . . . . . . . . . SEQUENCE {
 602  109: . . . . . . . . . . . . . . . SEQUENCE {
 604  107: . . . . . . . . . . . . . . . . SEQUENCE {
 606   39: . . . . . . . . . . . . . . . . . SEQUENCE {
 608   37: . . . . . . . . . . . . . . . . . . [6] 'voms1://testbed002.cnaf.infn.it:33334'
         : . . . . . . . . . . . . . . . . . . }
 647   64: . . . . . . . . . . . . . . . . . SEQUENCE {
 649   35: . . . . . . . . . . . . . . . . . . SEQUENCE {
 651    7: . . . . . . . . . . . . . . . . . . . OCTET STRING 'shortid'
 660    9: . . . . . . . . . . . . . . . . . . . OCTET STRING 'mycert2-g'
 671   13: . . . . . . . . . . . . . . . . . . . OCTET STRING '/voms1/group1'
         : . . . . . . . . . . . . . . . . . . . }
 686   25: . . . . . . . . . . . . . . . . . . SEQUENCE {
 688    7: . . . . . . . . . . . . . . . . . . . OCTET STRING 'shortid'
 697    7: . . . . . . . . . . . . . . . . . . . OCTET STRING 'mycert2'
 706    5: . . . . . . . . . . . . . . . . . . . OCTET STRING 'voms1'
         : . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . }
 713    9: . . . . . . . . . . . . SEQUENCE {
 715    3: . . . . . . . . . . . . . OBJECT IDENTIFIER '2 5 29 56'
 720    2: . . . . . . . . . . . . . OCTET STRING, encapsulates {
 722    0: . . . . . . . . . . . . . . NULL
         : . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . }
 724   31: . . . . . . . . . . . . SEQUENCE {
 726    3: . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . authorityKeyIdentifier (2 5 29 35)
 731   24: . . . . . . . . . . . . . OCTET STRING, encapsulates {
 733   22: . . . . . . . . . . . . . . SEQUENCE {
 735   20: . . . . . . . . . . . . . . . [0]
         : . . . . . . . . . . 90 E7 17 82 09 9B 3C DD 58 41 8C AB 8F C6 46 DB
         : . . . . . . . . . . 07 CA CD EE
         : . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . }
# The pk-cert-list extension (section 3.6.3)
 757  745: . . . . . . . . . . . . SEQUENCE {
 761   10: . . . . . . . . . . . . . OBJECT IDENTIFIER '1 3 6 1 4 1 8005 100 100 10'
 773  729: . . . . . . . . . . . . . OCTET STRING, encapsulates {
```

```
 777  725: . . . . . . . . . . . . . SEQUENCE {
 781  721: . . . . . . . . . . . . . . SEQUENCE {
 785  717: . . . . . . . . . . . . . . . SEQUENCE {
 789  566: . . . . . . . . . . . . . . . . SEQUENCE {
 793    3: . . . . . . . . . . . . . . . . . [0] {
 795    1: . . . . . . . . . . . . . . . . . . INTEGER 2
         : . . . . . . . . . . . . . . . . . . }
 798    1: . . . . . . . . . . . . . . . . . INTEGER 2
 801   13: . . . . . . . . . . . . . . . . . SEQUENCE {
 803    9: . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . md5withRSAEncryption (1 2 840 113549 1 1
4)
 814    0: . . . . . . . . . . . . . . . . . . NULL
         : . . . . . . . . . . . . . . . . . . }
 816   51: . . . . . . . . . . . . . . . . . SEQUENCE {
 818   11: . . . . . . . . . . . . . . . . . . SET {
 820    9: . . . . . . . . . . . . . . . . . . . SEQUENCE {
 822    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . countryName (2 5 4 6)
 827    2: . . . . . . . . . . . . . . . . . . . . PrintableString 'IT'
         : . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . }
 831   13: . . . . . . . . . . . . . . . . . . SET {
 833   11: . . . . . . . . . . . . . . . . . . . SEQUENCE {
 835    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . organizationName (2 5 4 10)
 840    4: . . . . . . . . . . . . . . . . . . . . PrintableString 'INFN'
         : . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . }
 846   21: . . . . . . . . . . . . . . . . . . SET {
 848   19: . . . . . . . . . . . . . . . . . . . SEQUENCE {
 850    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . commonName (2 5 4 3)
 855   12: . . . . . . . . . . . . . . . . . . . . PrintableString 'CAFromthisCN'
         : . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . }
 869   30: . . . . . . . . . . . . . . . . . SEQUENCE {
 871   13: . . . . . . . . . . . . . . . . . . UTCTime 03/11/2010 17:33:18 GMT
 886   13: . . . . . . . . . . . . . . . . . . UTCTime 05/11/2010 17:33:18 GMT
         : . . . . . . . . . . . . . . . . . . }
 901   27: . . . . . . . . . . . . . . . . . SEQUENCE {
 903   11: . . . . . . . . . . . . . . . . . . SET {
 905    9: . . . . . . . . . . . . . . . . . . . SEQUENCE {
 907    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . countryName (2 5 4 6)
 912    2: . . . . . . . . . . . . . . . . . . . . PrintableString 'IT'
         : . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . }
 916   12: . . . . . . . . . . . . . . . . . . SET {
 918   10: . . . . . . . . . . . . . . . . . . . SEQUENCE {
 920    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . commonName (2 5 4 3)
 925    3: . . . . . . . . . . . . . . . . . . . . PrintableString '003'
         : . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . }
 930  159: . . . . . . . . . . . . . . . . . SEQUENCE {
 933   13: . . . . . . . . . . . . . . . . . . SEQUENCE {
 935    9: . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . rsaEncryption (1 2 840 113549 1 1 1)
 946    0: . . . . . . . . . . . . . . . . . . . NULL
         : . . . . . . . . . . . . . . . . . . . }
 948  141: . . . . . . . . . . . . . . . . . . BIT STRING, encapsulates {
 952  137: . . . . . . . . . . . . . . . . . . . SEQUENCE {
 955  129: . . . . . . . . . . . . . . . . . . . . INTEGER
         : . . . . . . . . . 00 B0 D0 61 D2 46 67 17 EA 84 90 6F 35 F3 E7 50
         : . . . . . . . . . B8 21 D6 B7 99 0C 1C 32 29 95 48 EF 81 19 3F 08
         : . . . . . . . . . 8B E3 4D 77 76 42 8B 8C F8 BE 74 CC 30 FD E3 46
         : . . . . . . . . . B0 41 24 47 01 E3 EC 37 61 F8 1C 12 B5 48 08 A0
         : . . . . . . . . . 44 7A 73 29 47 21 4D 7D 44 C4 D5 7B 96 F9 6E 89
```

```
        : . . . . . . . . . EF 39 94 F0 95 B5 6F A1 7F E8 7D D7 6C 7D D7 FB
        : . . . . . . . . . 74 77 E5 0A 20 18 F4 DF E2 65 C7 B8 28 E5 97 5D
        : . . . . . . . . . B8 37 E7 F3 9D A7 BA B9 1C 3E 24 B9 D3 D4 9F F2
        : . . . . . . . . . . . . . [ Another 1 bytes skipped ]
1087    3: . . . . . . . . . . . . . . . . . . . . INTEGER 65537
        : . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . }
1092  263: . . . . . . . . . . . . . . . . . [3] {
1096  259: . . . . . . . . . . . . . . . . . . SEQUENCE {
1100    9: . . . . . . . . . . . . . . . . . . . SEQUENCE {
1102    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . basicConstraints (2 5 29 19)
1107    2: . . . . . . . . . . . . . . . . . . . . OCTET STRING, encapsulates {
1109    0: . . . . . . . . . . . . . . . . . . . . . SEQUENCE {}
        : . . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . . }
1111   70: . . . . . . . . . . . . . . . . . . . SEQUENCE {
1113    9: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . netscape-comment (2 16 840 1 113730
1 13)
1124   57: . . . . . . . . . . . . . . . . . . . . OCTET STRING, encapsulates {
1126   55: . . . . . . . . . . . . . . . . . . . . . IA5String
        : . . . . . . . . . 'OpenSSL Generated Certificate for VOMS testing p'
        : . . . . . . . . . 'urposes'
        : . . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . . }
1183   29: . . . . . . . . . . . . . . . . . . . SEQUENCE {
1185    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . subjectKeyIdentifier (2 5 29 14)
1190   22: . . . . . . . . . . . . . . . . . . . . OCTET STRING, encapsulates {
1192   20: . . . . . . . . . . . . . . . . . . . . . OCTET STRING
        : . . . . . . . . . 90 E7 17 82 09 9B 3C DD 58 41 8C AB 8F C6 46 DB
        : . . . . . . . . . 07 CA CD EE
        : . . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . . }
1214  129: . . . . . . . . . . . . . . . . . . . SEQUENCE {
1217    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . authorityKeyIdentifier (2 5 29 35)
1222  122: . . . . . . . . . . . . . . . . . . . . OCTET STRING, encapsulates {
1224  120: . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1226   20: . . . . . . . . . . . . . . . . . . . . . . [0]
        : . . . . . . . . . A7 DB C2 A3 F9 3D FB D5 37 CC EE 46 21 57 44 36
        : . . . . . . . . . E2 E3 A2 71
1248   93: . . . . . . . . . . . . . . . . . . . . . . [1] {
1250   91: . . . . . . . . . . . . . . . . . . . . . . . [4] {
1252   89: . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1254   11: . . . . . . . . . . . . . . . . . . . . . . . . . SET {
1256    9: . . . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1258    3: . . . . . . . . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . . . . . . . . countryName (2 5 4 6)
1263    2: . . . . . . . . . . . . . . . . . . . . . . . . . . . PrintableString 'IT'
        : . . . . . . . . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . . . . . . . . }
1267   11: . . . . . . . . . . . . . . . . . . . . . . . . . SET {
1269    9: . . . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1271    3: . . . . . . . . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . . . . . . . . stateOrProvinceName (2
5 4 8)
1276    2: . . . . . . . . . . . . . . . . . . . . . . . . . . . PrintableString 'IT'
        : . . . . . . . . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . . . . . . . . }
1280   14: . . . . . . . . . . . . . . . . . . . . . . . . . SET {
1282   12: . . . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1284    3: . . . . . . . . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
        : . . . . . . . . . . . . . . . . . . . . . . . . . . . . localityName (2 5 4 7)
1289    5: . . . . . . . . . . . . . . . . . . . . . . . . . . . PrintableString 'THISL'
        : . . . . . . . . . . . . . . . . . . . . . . . . . . . }
        : . . . . . . . . . . . . . . . . . . . . . . . . . . }
1296   13: . . . . . . . . . . . . . . . . . . . . . . . . . SET {
1298   11: . . . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
```

```
1300    3: . . . . . . . . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . . . . . . . . organizationName (2 5
4 10)
1305    4: . . . . . . . . . . . . . . . . . . . . . . . . . . . PrintableString 'INFN'
         : . . . . . . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . . . . . . }
1311   13: . . . . . . . . . . . . . . . . . . . . . . . . . SET {
1313   11: . . . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1315    3: . . . . . . . . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . . . . . . . . organizationalUnitName
(2 5 4 11)
1320    4: . . . . . . . . . . . . . . . . . . . . . . . . . . . PrintableString 'INFN'
         : . . . . . . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . . . . . . }
1326   15: . . . . . . . . . . . . . . . . . . . . . . . . . SET {
1328   13: . . . . . . . . . . . . . . . . . . . . . . . . . . SEQUENCE {
1330    3: . . . . . . . . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . . . . . . . . commonName (2 5 4 3)
1335    6: . . . . . . . . . . . . . . . . . . . . . . . . . . . PrintableString 'thisCN'
         : . . . . . . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . . . }
1343    1: . . . . . . . . . . . . . . . . . . . . . . [2] 01
         : . . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . }
1346   11: . . . . . . . . . . . . . . . . . . . SEQUENCE {
1348    3: . . . . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . . . . keyUsage (2 5 29 15)
1353    4: . . . . . . . . . . . . . . . . . . . . OCTET STRING, encapsulates {
1355    2: . . . . . . . . . . . . . . . . . . . . . BIT STRING 5 unused bits
         : . . . . . . . . . . . . . . . . . . . . . . '111'B
         : . . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . . . }
1359   13: . . . . . . . . . . . . . . . . SEQUENCE {
1361    9: . . . . . . . . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . . . . . . . . md5withRSAEncryption (1 2 840 113549 1 1
4)
1372    0: . . . . . . . . . . . . . . . . . NULL
         : . . . . . . . . . . . . . . . . . }
1374  129: . . . . . . . . . . . . . . . . BIT STRING
         : . . . . . . . . . 1A 9B 98 6B 51 14 36 EB 5D 75 5F 3E F0 05 76 D2
         : . . . . . . . . . EB 8D B9 2C F3 4D 5A 79 EA 40 44 39 F4 DB 95 65
         : . . . . . . . . . 3A C1 2B 5F 99 17 91 0D EE E2 B3 16 AD 28 0E 15
         : . . . . . . . . . F8 44 DC A7 09 3C 8A 82 0B 3B 85 D4 B2 48 48 7E
         : . . . . . . . . . 2C D1 52 C7 AB C3 0D 04 A6 E6 D8 DF A2 89 EF 5E
         : . . . . . . . . . 3E 1A 70 46 01 78 43 6A 62 4B 37 C8 92 CA C5 3B
         : . . . . . . . . . A8 4F 5F 81 B2 10 EA AF 5F 74 71 46 65 F4 60 2F
         : . . . . . . . . . 7A 0F D9 D8 E0 67 70 1C 6F 5A 94 54 A8 04 25 46
         : . . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . . }
         : . . . . . . . . . . . . . }
         : . . . . . . . . . . . . }
         : . . . . . . . . . . . }
         : . . . . . . . . . . }
1506   13: . . . . . . . . . SEQUENCE {
1508    9: . . . . . . . . . . OBJECT IDENTIFIER
         : . . . . . . . . . . . md5withRSAEncryption (1 2 840 113549 1 1 4)
1519    0: . . . . . . . . . . NULL
         : . . . . . . . . . . }
1521  129: . . . . . . . . . BIT STRING
         : . . . . . . . . . 70 DF 83 7E 5A 87 D7 07 45 66 4A 2F 23 18 97 11
         : . . . . . . . . . 3A 83 0F 2A 3B 42 75 00 C9 FB E5 53 6F 0B 16 5D
         : . . . . . . . . . 7C E9 68 49 1E 67 4B AF 50 51 56 89 3F 80 AC 04
         : . . . . . . . . . 95 27 8F CA C8 AD 11 14 1A 4B B2 40 7F 98 D9 65
         : . . . . . . . . . . 5E 42 2F D6 95 A2 D5 C5 E0 0C E8 E7 A8 58 1C 18
         : . . . . . . . . . . E6 61 7E A1 98 40 2F B8 65 8E C1 63 A0 CE 24 B1
         : . . . . . . . . . . 5F 37 C2 09 3C 32 00 39 21 67 63 8F 35 1A 8F 1B
         : . . . . . . . . . . 3B BA E9 DF 97 ED 8F BE 4F 86 9B 47 C9 9D 5A F3
         : . . . . . . . . . }
         : . . . . . . . . }
         : . . . . . . . }
         : . . . . . . }
         : . . . . . }
1653   14: . . . . SEQUENCE {
1655    3: . . . . . OBJECT IDENTIFIER keyUsage (2 5 29 15)
1660    1: . . . . . BOOLEAN TRUE
1663    4: . . . . . OCTET STRING, encapsulates {
1665    2: . . . . . . BIT STRING 4 unused bits
         : . . . . . . . '1101'B
         : . . . . . . }
         : . . . . . }
1669   16: . . . . SEQUENCE {
1671   10: . . . . . OBJECT IDENTIFIER '1 3 6 1 4 1 8005 100 100 6'
1683    2: . . . . . OCTET STRING 30 33
         : . . . . . }
1687   29: . . . . SEQUENCE {
1689    8: . . . . . OBJECT IDENTIFIER '1 3 6 1 5 5 7 1 14'
1699    1: . . . . . BOOLEAN TRUE
1702   14: . . . . . OCTET STRING, encapsulates {
1704   12: . . . . . . SEQUENCE {
1706   10: . . . . . . . SEQUENCE {
1708    8: . . . . . . . . OBJECT IDENTIFIER '1 3 6 1 5 5 7 21 1'
         : . . . . . . . . }
         : . . . . . . . }
         : . . . . . . }
         : . . . . . }
         : . . . . }
         : . . . }
         : . . }
1718   13: . SEQUENCE {
1720    9: . . OBJECT IDENTIFIER md5withRSAEncryption (1 2 840 113549 1 1 4)
1731    0: . . NULL
         : . . }
1733  129: . BIT STRING
         : . . . 61 D7 C1 1B 11 7B 4D 96 B8 7F 78 36 F8 DE BD D7
         : . . . 17 DB EA A5 DF C9 78 27 09 39 C7 83 8A 43 E1 F7
         : . . . DA 08 36 7B 29 84 2A EB 73 25 A5 7B 5E 43 A0 C0
         : . . . 64 62 41 BE 6B 9B 5C 83 CF 75 24 5C A0 65 6F A4
         : . . . 74 42 F2 DB D8 1A D9 20 C8 65 10 92 ED 1A A2 49
         : . . . 5A 30 C3 99 15 F6 D4 42 3C E3 EB EC 55 F5 9F 20
         : . . . 67 7A DC B5 44 4F 09 F4 3A 79 FA 52 68 7F 18 81
         : . . . 72 21 8A 00 BB 08 7A 49 6D AD 19 38 77 CC 96 E4
         : . }
```

6. Security Considerations

This specification defines the elements and use of attributes for authorization services. Implementers of attributes need to be aware that errors in implementation could lead to denial of service or improper granting of service to unauthorized users. Users of attribute assertions should be aware of the situations in which they must require and verify signed assertions.

The following issue should in particular be noted:

- If the contents of the IssuerCerts (section 3.6.3) extension is used to validate the signature of the AC, than the validating entity needs independent confirmation that the certificate retrieved from the extension is indeed authorized to sign ACs for that specific VO. There are several ways to do this.

Author Information

Valerio Venturi
INFN – CNAF
Viale Berti Pichat, 6/2
I – 40127 BOLOGNA
valerio.venturi@cnaf.infn.it

Vincenzo Ciaschini
INFN - CNAF
Viale Berti Pichat, 6/2
I - 40127 BOLOGNA
vincenzo.ciaschini@cnaf.infn.it

Intellectual Property Statement

Full Copyright Notice

Normative References

[RFC5280] D. Cooper, S. Santesson, S. Farrel, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" RFC5280, May 2008

[RFC3820] S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson, “Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile”, RFC 3820, June 2004

[RFC5755] S. Farrell, R. Housley, S. Turner, “An Internet Attribute Certificate Profile for Authorization”, RFC 5755, January 2010.

Informational References

[VOMS1] "VOMS Architecture v1.1," http://grid-auth.infn.it/docs/VOMS-v1_1.pdf, February 2003.

[OGSI-Authz-Attrs] Thompson, M., Welch, V., Lorch, M., Lepro, R., Chadwick, D., Ciaschini V. “Attributes used in OGSA Authorization”, GWD-57.