GFD-C
Category: Community Practice Documents
CA Operations WG

Michael Helm, ESnet/LBL
Tony J. Genovese, ESnet/LBL

March 5, 2003

Common Grid Certificate Authority Names and Naming

Status of This Memo

This memo provides information to the Grid community on common naming practices for Certificate Authorities. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Abstract

Grid Certificate Authorities (CA) must each decide on a set of names and publishing points. To facilitate deployment and ease of discovery a proposed common set these names are specified below. The naming principles used to construct them are also described. Some additional naming fields, such as SubjectAltName, are also specified with optional (and non-exclusive) values. Other protocols such as HTTP, FTP, and SMTP, may be used to access CA resources, and a naming convention for CA objects is described.

Table of Contents

1 Principles

Base names should be globally recognized

- CA's will have wide recognition and use
- Need impartial naming conflict resolution
- Well understood problem in X.500/LDAP

Relying parties can find CA objects easily

- SRV and other location protocols don't cover our problems completely

Use CA certificate contents to derive access information

- The certificate may not contain every possible extension and URI/URL
- The subject name should be enough to derive other possible access points

Naming must work with existing software

Directory (LDAP) naming is fundamental

- Directory Names drive the structure
- Subject names and not other components are used

1.1 Discussion

Subject base names need to be based on a well-recognized naming scheme. X.500 [X501] proposed a world-wide DIT based on Organization and Country names, e.g. O=ESnet, C=US. This depended on a registrar to act for the "C=US" branch. For some years this duty was shared between the US Government and ANSI; in other countries, appropriate organizations managed a registrar. This system never quite worked and has now failed completely in most places. Another scheme has been evolving in the IETF, depending on Domain Components, which are related to Internet DNS names, e.g. DC=ES, DC=net compared to "es.net". This scheme is not completely standardized, but the domain naming system (DNS) is a reasonable foundation. DNS is reliable, everyone has a very high stake in making sure the DNS continues to work, its names have some legal recognition as an organization marker, and there is a dispute resolution process. It is not feasible to invent another global naming system that at best duplicates what can be had from DNS.

However, these Domain Component names have to work. This scheme has been tested with GT2 and found to work properly. Openssl, the underlying certificate handling API in GSI, still has some problems with DC naming, but these problems seem to be confined to representation. However we have found several classes of Netscape or IPlanet products that require an "O=" attribute value assertion, otherwise the products fail (dump core or exit). The most affected product is the Netscape 4.7x browser. We assume we will have to support that browser for several more years. Study showed that the root CA signing certificate was the critical certificate; this certificate needed to have an "O =" component. Therefore we are adding "O=ESnet" to the root CA subject. Since ESnet registered its name with ANSI years ago as part of its X.500 service, ESnet has a good claim to ownership and so inserting it into its namespace should be acceptable.

We are not ready to install a large number of objects in CA certificates. In some cases these extensions would be undesirable, and in others the decision about how to do them requires flexibility (something one doesn't have with a CA signing certificate). Customers and relying parties still need to find objects: CRL's, CP documents, certificates of various kinds, and services. Therefore, creating a consistent pattern for building and finding these objects as needed is useful. We do not guarantee that any or all of these references will actually exist. Their existence is determined by the CA's particular specification and by its CPS.

At the time of publication, the IETF LDAPBIS and PKIX working groups are resolving the use of the ";*binary*" transfer option attached to the attribute name of certain certificate types. Since this option is used (and probably required) by LDAP clients and servers in current use, it will usually be shown in the examples below. It appears from the discussion in these groups that this transfer option will not continue as part of the standard and will be dropped as vendor updates permit.

2 Canonical Representation

<Basename> is represented as appropriate for the particular representation, eg DC=name, DC=topname for LDAP/X.500 names; name.topname for DNS.
<Descriptive name> is expected to be a string or phrase like "Lawrence Berkeley Lab". Descriptive names are shown with blanks and other non-alphanumeric characters here, in the interest of legibility. They may also be shown with the appropriate syntax for the protocol, including escape character construction as appropriate from[GT2AG]
"Globus 2.2 Admin Guide", Globus, 2002, http://www.globus.org/gt2.2/admin/index.html
[RFC1738] and [RFC1959]. Spaces are replaced by "-"in email addresses.

2.1 Short Names and HTML

The Directory (LDAP) is fundamental to the naming structure used, and certificate subject names are mapped to other services. Since the values of some of these components is so long, and their abbreviations universally undersood, the abbreviations are used in other services. In particular these abbreviations are preferred in web servers. Both long and short forms should be supported.
The intent is to provide identical paths, such that
/DC=org/DC=BigLab/OU=Certificate Authorities/CN=BigLab CA 1
would translate to
CN=BigLab CA 1, OU=Certificate Authorities, DC=BigLab, DC=org [LDAP]
… and to something like
http://biglab.org/DC/org/DC/BigLab/OU/Certificate Authorities/CN/BigLab CA 1
Since the structure of names is fairly rigid, in that the order of components, the component type, and name, are restricted, it is acceptable to omit the LDAP attribute value names entirely and most of the LDAP components in some services, eg HTTP paths or FTP file systems. For example, it is assumed that the server DNS name will usually reflect the "Domain Component" portion of the path. A Certificate Authority entity would only appear under "OU=Certificate Authorities". It is acceptable to use the abbreviation "CA" for the entire OU component.
Services may use any combination of acceptable name forms, but the simplified URL's for http shown below should be used.

2.2 Abbreviations

These names and strings are considered equivalent. When one of these names is used in a name component, it is expected that the equivalent long form or abbreviation will both be provided for the benefit of naïve users conducting searches. For example, "Certificate Authority" and "CA", as used in HTTP and LDAP names below.

- Certificate Revocation List = CRL
- Descriptive Name = DesName
- Certificate Policy = CP ***[RFC2459]***
- Certification Practices Statement = CPS ***[RFC2459]***
- Certificate Authority = Certificate Authorities = CA
- End Entity Name = EEName

2.3 Subject name

CN=<DesName>, OU=CA, <basename>

2.4 Subject Alternative Name (SubjectAltName)

2.4.1 RFC822

<DesName>@<basename>

2.5 End Entity

[Specification left to CP/CPS]

2.5.1 LDAP

The directory entries should be found in the domain's standard directory server. DNS SRV records should take precedence naming the hosts where these directories could be found below.

2.5.1.1 Issuer

Entity name

ldap://{ldap.}<basename>/ CN= <DesName>, OU=CA, <basename>

Entity attribute value assertions

See [RFC2587] for information on this LDAP attribute.
CA certificate: cACertificate: <attribute value>
Access points should be visible as URL attributes here. "Access points" are user interfaces.

In LDAP URL [RFC1959] format:
ldap://{ldap.}<basename>/ CN= <DesName>, OU=CA, <basename>?cACertificate

In LDIF [RFC2849] format:

```
  dn:  CN= <DesName>, OU=CA, <basename>
    …
  cACertificate;binary : <encoded value>
```

2.5.1.2 Certificate Revocation List

CRL Issuing Point:

In the Issuer's entry:
ldap://{ldap.}<basename>/ CN= <DesName>, OU=CA, <basename>

CRL

Attribute of Issuer (above)
certificateRevocationList: <attribute value>
See [RFC2587] for information on this LDAP attribute.

In LDAP URL format:

ldap://{ldap.}<basename>/ CN= <DesName>, OU=CA, <basename>? certificateRevocationList

In LDIF format:

```
dn:  CN= <DesName>, OU=CA, <basename>
    …
certificateRevocationList;binary : <encoded value>
```

2.5.2 HTTP

2.5.2.1 Issuer Certificate

http://{www.} <basename>/CA/<DesName>
<HASH> [e.g.: "9d8753eb"]

This "page" is a directory; it should provide content such as CA's signing certificate, as <DesName>.cer, <DesName>.txt -- see below for other content.
It is assumed below that both the descriptive name form and the hash name form of the CA are provided, and that both directories are identical in content.

2.5.2.2 Access point

Subscriber and agent UI should be visible in obvious form at
http://{www.}<basename>/CA/<DesName>
Other URL formats or protocols may also be used. Subscriber and agent UI should both be visible.
ACL's may be used to restrict visibility.

2.5.2.3 CP/CPS

http://{www.}<basename>/CA/ <DesName>/ CP.{doc,pdf}
[Question: how to show link to OID? OID.{doc,pdf}->CP?]
[Question: how to indicate multiple policies]
CPS.{doc,pdf}
[Note same questions apply here as above]

2.5.2.4 CRL

http://{www.}<basename>/CA/ <DesName>/ <Descriptive Name>.crl
http://{www.}<basename>/CA/<HASH>/<HASH>.crl

2.5.2.5 Certificates

http://{www.}<basename>/CA/ <DesName>./{People,…}/<certificate hash value>

2.5.2.6 Registration Authority

http://{www.}<basename>/RA
http://{www.}<basename>Registration Authority
Contents to be determined by CA management
http://{www.}<basename>RA.txt - short descriptive list of RA entities, in format determined by CA management

2.5.3 FTP

ftp://{ftp.}<basename>/ CA/<DesName>/
<HASH>/
Mirror the web structure.

2.5.4 SMTP

<DesName>@<basename>/

3 Notes

Related names will also be linked, e.g.
"Certificate Authorities" = "CA" = "ca" = "certificate authorities" = "certificate authority" = "Certificate-Authorities" &c
"CRL" = "Certificate Revocation List"
Certificates may or may not be published to a web server or LDAP server; that decision will be specified in the CPS.
Specification of end entity certificates is in the CA's CPS.

Specification of an alternative directory name for the root CA may allow us to simplify the root CA's issuer name in the future (see [RFC2459] and [RFC3280]).

Author Information

Michael Helm
One Cyclotron Road
Berkeley, CA USA 94706

Tony J. Genovese
One Cyclotron Road
Berkeley, CA USA 94706

Glossary

- **CRL** – Certificate Revocation List
- **DIT** – Directory Information Tree – hierarchy of LDAP entities
- **End Entity** – a customer, a computer host, a service; other uses possible
- **Base name**
- **Suffix** – the local "root" of an LDAP DIT
- **CA Namespace** – in the Grid environment (one based on GSI), CA's sign in well-defined namespaces. This namespace is approximately (usually exactly) equal to the base name or suffix, or small set of suffixes. A CA can sign in more than one namespace.

Intellectual Property Statement

The GGF 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 GGF Secretariat.

The GGF 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 GGF Executive Director.

Full Copyright Notice

References

[GT2AG]

“Globus 2.2 Admin Guide”, Globus, 2002, http://www.globus.org/gt2.2/admin/index.html

[RFC1738]

“Uniform Resource Locators (URL)”, Berners-Lee & al, IETF, 1994, http://www.ietf.org/rfc/rfc1738.txt

[RFC1959]

“An LDAP URL Format”, Howes & al, IETF, 1996, http://www.ietf.org/rfc/rfc1959.txt

[RFC2849]

“The LDAP Data Interchange Format (LDIF) - Technical Specification”, Good, IETF, 2000, http://www.ietf.org/rfc/rfc2849.txt

[RFC2459]

“Certificate and CRL Profile”, Housely &al, PKIX, IETF, 1999, http://www.ietf.org/rfc/rfc2459.txt

[RFC2587]

“LDAPv2 Schema”, Boyen &al, PKIX, IETF, 1999, http://www.ietf.org/rfc/rfc2587.txt

[RFC2849]

“The LDAP Data Interchange Format (LDIF) - Technical Specification”, Good, IETF, 2000, http://www.ietf.org/rfc/rfc2849.txt

[RFC3280]

“Certificate and Certificate Revocation List (CRL) Profile”, Housely &al, PKIX, IETF, 2001, http://www.ietf.org/rfc/rfc3280.txt