GFD-C
Category: Community Practice Documents
CA Operations WG

Michael Helm, ESnet/LBL

March 5, 2003

Grid Certificate Extensions Profile

Status of this Memo

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

Copyright Notice

Abstract

Standard usage of X.509 certificate attributes and extensions will promote the interoperability of grid infrastructures. Relying parties will be better able to understand certificate policy documents, and be in a better position to make trust decisions about certificate authorities. Aligning grid CA practices with industry practice may allow existing PKI's, or PKI's now developing independently, to use grid infrastructures, and grid certificates to be used in other applications. Accordingly, standardization of certain attributes and extensions of X.509 v3 certificates is discussed. An appendix describes some existing infrastructures.

Table of Contents

1 Introduction

X.509 certificates consist of a standard set of fields, one of which is a sequence of extensions. Extensions, in turn, are divided into a standard set pre-defined in [X509v3], and private extensions. The usage of certificate fields and extensions in the grid is tacitly bound to the IETF PKIX profile (see Author Information

Michael Helm
One Cyclotron Road
Berkeley, CA USA 94720
Helm@es.net

Glossary

TBD

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

[RFC2459] and ***[RFC3280]***). However, the PKIX profile allows a wide latitude for usage, and grid usage may require additional private extensions and customizations, as has been described elsewhere.

In this document we consider how the existing set of well-known fields and extensions can be used in the grid, and how usage should align with practice observed in other PKI's. We would like to arrive at a common understanding of what certain extensions mean, how they are or could be used, and recommendations for relying parties and certificate authority operators.

[[Problems: Automatic interpretation of certs; policy; correct fields in certs; End-Entity vs CA vs other usage]]

What are the useful and acceptable extensions – values – ranges for a grid Certificate Authority or issuer certificate? Typical end entity certificates: people, services, SSL servers?

2 X.509 Certificate Extensions

2.1 X.509 Certificate Fields

The usage of most fields has been established by standards document and by custom. Perhaps this should be out of scope. Possibilities include:

2.1.1 Serial Number

[[Format? Expectations?]]

2.1.2 Subject

Are there structural or component issues with names? Should names be based in an unambiguous name space (eg DNS)? Are there any issues with the use of certain components in the name?

2.1.3 Subject Public Key Info

Algorithm? RSA is in most common use – what about other algorithms – eg, could DSA be used in our environment?

2.1.4 Issuer Unique ID

Do we include or care?

2.1.5 Subject Unique ID

Do we include or care? Deprecated by RFC 2459

2.2 X.509 Certificate Extensions

2.2.1 Standard Extensions

2.2.1.1 Authority Key Identifier

A unique identifier of the key that should be used in verifying the certificate; for all certs except self-signed

2.2.1.2 Subject Key Identifier

RFC 2459: Mandatory for CA; optional for EE.

2.2.1.3 Key Usage

This is crit ical for both CA's (RFC 3280) and EE certs.

2.2.1.4 Extended Key Usage

This is where "TLS server" would appear. There are several OIDs specified in RFC 3280 for this.

2.2.1.5 CRL Distribution Point

[[There are some uses of this that I don't understand. It is an extension designed to be applied by the CA to the signed cert; there appear to be provisions for describing multiple CRL signers and locations, delta CRL's, and CRL extensions or types. Putting CRL info into EE certs does not seem very useful in the grid environment; perhaps discussion of the AIA extension OCSP option (see 2.2.2.1 below) in tandem is appropriate.]]

2.2.1.6 Private Key Usage Period

2.2.1.7 Certificate Policies

If we are ever going to implement policies such as "levels", and policy mapping, we will have to insert policy oids in our certificates. [[Subject to discussion]]

2.2.1.8 Policy Mappings

This extension is only present in CA certificates or cross-signing certs, maps policy oids together.

2.2.1.9 Subject Alternative Name

For S/MIME, an email address (RFC822 name). It is not clear whether adding the DNS name of hosts or "servers" to the certificate will be of much benefit, either in a grid or SSL environment.

2.2.1.10 Issuer Alternative Name

A sequence of alternative name forms for the issuer: DN, email address &c.

2.2.1.11 Subject Directory Attributes

Probably outdated

2.2.1.12 Basic Constraints

RFC 2459 recommends this be used in CA certificates only, and RFC 3280 further clarifies this. This extension includes a Path Length Constraint, which cannot be used at the present time in grids.

2.2.1.13 Name Constraints

This extension, which exists only in CA certificates, indicates allowed or excluded names from the CA's signing name space. This constraint is applied to both Subject field and Subject Alternative Name extension. It is completely unusable in the grid due to limitations of OpenSSL.

2.2.2 Private Extensions

2.2.2.1 Authority Information Access

This extension, defined by RFC 2459, has two defined OIDs: One points to information about CA issuers higher on the hierarchy than the issuer of this certificate. The other defines a URI for access to OCSP services. The OCSP responder is URI is described by RFC 2560. There are a few examples of its use in the data collection.

2.2.2.2 Subject Information Access

This private extension was added by RFC 3280 for internet use. There are no examples of its usage in the data collection, but the description from RFC 3280 section 4.2.2.2 is intriguing:

> The subject information access extension indicates how to access information and services for the subject of the certificate in which the extension appears. When the subject is a CA, information and services may include certificate validation services and CA policy data. When the subject is an end entity, the information describes the type of services offered and how to access them.

This extension merits further discussion, perhaps in tandem with ESnet's naming paper.

2.2.3 Custom Extensions

3 X.509 CRL Extensions

[[To be added if interest warrants.]]

4 Security

Security issues are integral to the use of X.509 certificates, revocation lists, and extensions. Security considerations are discussed in each item.

Author Information

Michael Helm
One Cyclotron Road
Berkeley, CA USA 94720
Helm@es.net

Glossary

TBD

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

[RFC2459]
Housely &al, “Certificate and CRL Profile”, PKIX, IETF, 1999, http://www.ietf.org/rfc/rfc2459.txt

[RFC3280]
Housely &al, “Certificate and Certificate Revocation List (CRL) Profile”, PKIX, IETF, 2001, http://www.ietf.org/rfc/rfc3280.txt

A Certificate Extensions

[[Certificate examples gathered from the field; the contents of the earlier paper]]