GWD-R.225
CAOPS-WG
davidg@nikhef.nl,
mike.jones@jisc.ac.uk,
jens.jensen@stfc.ac.uk

David L. Groep, Nikhef*
Mike Jones, Jisc*
Jens Jensen, RAL/STFC*
Michael Helm, LBNL/ESNet
Milan Sova, CESNET
Scott Rea, DigiCert Inc.
Reimer Karlsen-Masur, DFN-CERT
Ursula Epting, KIT
March 2016

Interoperable Certificate Profile

Status of This Document

This document provides **recommendations** to the OGF community.

Obsoletes

This document supersedes GFD.125 [1].

Copyright Notice

Dedication

This work is dedicated to the memory of our co-author, collaborator, and friend, Milan Sova.

Abstract

This document provides guidance for the use of directory names, attributes, and extensions in X.509 certificates, such that they are usable by the majority of the infrastructures supported by IGTF today—these used to be exclusively grids but are now more general e-infrastructures and cyberinfrastructures. The intended audience for this document includes issuers of X.509 certificates for use in such infrastructures, and implementers of associated X.509 validation software.

Interoperability for X.509 identity certificates between the issuers of certificates and the software that interprets them is becoming increasingly important as the number of participants in infrastructures that rely on a X.509 certificates grows. It is difficult to predict which particular software will be used by the parties relying on the certificate, and how this software interprets specific name

forms, attributes, and extensions. This document gives guidance and defines explicit restrictions on the certificate profile (*i.e.*, the type of names and encoding of names and extensions in certificates) to ensure that the certificate is interpreted by the relying party in the way the issuer intended. It specifies and further restricts the certificate format as defined in RFC 5280 [2] and the X.509 standard [3].

This document supersedes the guidance in GFD.125 [1] by specifying additional constraints and providing further clarification. Also, where GFD.125 provided *guidance*, this document provides *recommendations*.

Contents

1 Scope of this document

This document provides guidance for the use of attributes and extensions in X.509 [3] certificates such that the certificates are usable by the majority of the IGTF infrastructures today (www.igtf.net). This guidance must be interpreted in the context of RFC 5280 [2], *i.e.*, all certificates must also be compliant with RFC 5280 in addition to any limitations imposed by the guidelines in this document[1].

Specific attention has been given to the representation of the subject and issuer distinguished names as strings, since in much of the software in infrastructures supported by the IGTF it is this string rendering, and not the actual sequence of relative distinguished names, which is used for identification and subsequent authorization purposes. This imposes specific additional constraints on such names, and on the set of attributes which can be used in these names, to ensure wide interoperability of the certificates.

If a particular extension or attribute is not discussed in this document, this should not be construed as meaning the extension or attribute is either harmless or useful; it means that at the time of writing it was not in widespread use, and was therefore not needed for interoperability. It may or may not be harmless and may or may not cause interoperability problems. It is recommended that specific interoperability testing is performed prior to including any such extensions or attributes.

Notational Conventions

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "REQUIRED", "SHALL", "SHALL NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [4].

[1] If RFC 5280 and this document contradict each other, this document takes precedence.

2 Self-signed and subordinate Certification Authority certificates

2.1 General provisions

All Certification Authority (CA) certificates MUST be in X.509 version 3 format, *i.e.*, the version number MUST be set to the value "2", as the use of specific extensions such as basicConstraints and keyUsage is required.

2.2 Serial Number

The serial number of each CA certificate SHOULD be unique among all certificates representing that CA[2].

If the end-entity certificates include an authorityKeyIdentifier extension with the issuer's serial number, the serial number SHOULD remain the same on re-issuing the CA certificate if continued validation of such end-entity certificates is desired[3]. Note that including the attribute serial number in authorityKeyIdentifier extension in end-entity certificate is strongly discouraged (section 3.4.7).

2.3 Issuer and Subject names

Only a limited number of attribute types are well supported by all of the current relying party software implementations when used as part of the Issuer or Subject Distinguished Name (DN). Therefore, only the following attribute types SHOULD be used, as they can be considered "safe": *domainComponent* (DC), *countryName* (C), *stateOrProvinceName* (ST), *localityName* (L), *organisationName* (O), *organisationalUnitName* (OU) and *commonName* (CN). Other attributes in distinguished names may result in incompatible representations, and thus SHOULD NOT be used.

To ensure uniqueness and reproducibility of the string renderings of DNs, each RelativeDistinguishedName (RDN) MUST contain an ASN.1 SET of length 1. Other SET lengths MUST NOT

[2]If a root or intermediate CA certificate is re-issued with the same serial number—for example in the case that only the lifetime is extended but the key pair remains the same—web browsers using the Mozilla NSS code base will issue a user warning and the import will fail (tested in Spring 2007), but if installation of the new certificate is attempted in Microsoft Internet Explorer it will overwrite the old one (tested in versions up to and including version 6). For Internet Explorer 7 and later (and verified up to IE version 9), both certificates will be in the trust store, but the most recently imported certificate will always be used. Thus, for NSS-based browsers the old certificate has to be removed from the certificate store first,and for IE7+ removing the earlier certificate first is advised as well.

[3]Note that if this is done the extended CA certificate will fail to import or validate in most client software that has stored or cached the previous version of such a CA certificate

be used.

Contrary to what may be deduced from the guidance given in X.521, multiple instances of the *organisationName* attribute MAY be used in a single DN. It has been confirmed by experience that all known software used in (grid, or similar) infrastructure deployments as of this writing correctly handles their representation, and will collate the attributes in the proper order. Also, multiple instances of the *commonName* attribute MAY be used.

Note, however, that the visual rendering of a multiple *organisationName* (O) or *commonName* (CN) attributes in many browsers may not be complete, and usually only the first or the last of these is displayed to the user. This only affects the visual representation, since the known infrastructure middleware uses the entire DN for subject identification. If no O or OU attributes appear in the DN, browsers[4] might not use other components to show affiliation.

String encoding of the RDN components

The DN is usually made up of a combination of the RDN types "DC", "C", "ST", "L", "O", "OU" and "CN". These components in distinguished names, with the exception of "DC," MUST be compliant with RFC 4630 [5] and SHOULD[5] be encoded as PrintableString; if not using PrintableString, they MUST be encoded using UTF-8 using only the PrintableString subset of characters[6], as per RFC 4630. The "DC" attribute MUST be encoded as IA5String. See section 4.3 for the details.

Issuer and authority subject name RDN component recommendations	
Required	*commonName*
Advised to use	*domainComponent*, *organisationName*
Optional	*countryName*, *stateOrProvinceName*, *localityName*, *organisationalUnitName*
MUST NOT be used	*serialNumber*, *emailAddress*, *userID* (also known as 'uid'), *uniqueIdentifier* (also known as 'uid'), *streetAddress*, *postalCode*

2.3.1 *commonName*

The *commonName* SHOULD be used in the subject distinguished name of a CA root certificate, as it allows easy visual recognition of the CA name. As the CN of the subject DN is often the most prominently displayed name of the CA, the CN SHOULD be a descriptive explicit string

[4] In particular this applies to browsers based on the Mozilla NSS code base.

[5] recommendation due to limitations in current implementations

[6] Some older jglobus libraries do not calculate the correct issuer hash unless all Issuer RDNs are encoded as printableString.

distinguishing the authority's name[7]. In addition the use of the "O" entry is encouraged, as it, too, is likely to be displayed.

2.3.2 *domainComponent*

To ensure uniqueness and proper authoritative identification, it is strongly encouraged to use *domainComponent* (DC) naming at the beginning of both issuer and subject DN, based on a DNS name registered to the organisation responsible for the CA.

In that case, the ASN.1 SEQUENCE MUST start with the *domainComponent* representing the top-level domain, for example "`DC=org`" or "`DC=eu`".

domainComponent MUST be encoded as an IA5String, see 4.3.

2.3.3 *countryName*, *stateOrProvinceName*, *localityName*, *organisationName*, *organisationalUnitName*

If the *countryName* (C) attribute is used, the value of this attribute SHOULD contain the two-letter ISO 3166 [6] encoding of the country's name[8,9]. The *countryName*, if used, MUST be used at most once.

Any of the *stateOrProvinceName* (ST), *localityName* (L), *organisationName* (O), and *organisationalUnitName* (OU) attributes MAY be used and SHOULD be used in the intended X.501 sense.

The use of at least one descriptive *organisationName* (O) attribute in the DN is RECOMMENDED.

[7] Having a *commonName* of just "CN=CA" will result in the display name of the CA in many browsers to show just the string 'CA' as the name, which may result in confusion.

[8] The designation UK is an well-known exception, mainly for historical reasons—GB is the official ISO 3166-1 representation for the United Kingdom of Great Britain and Northern Ireland, although in many contexts the designation "UK" is used for the same. Either GB and UK MAY be used as designations. Note that the Ukraine MUST be encoded as UA.

[9] In case the *countryName* (C) is used as part of the varying part of the subject distinguished name (i.e., it is not part of the constant DN prefix that defines the issuing namespace), the *countryName* (C) asserted in the subject DN of an end-entity certificate SHOULD correspond the home country of the end-entity, and thus does not necessarily reflect and is not necessarily the same as the country in which the CA is operating, or the country code in the issuer DN. Therefore, in such cases the *countryName* attribute SHOULD NOT be part of a subject DN naming prefix.

2.3.4 *serialNumber*

The attribute type *serialNumber* {2.5.4.5} MUST NOT be used in any Name[10].

2.3.5 *emailAddress*

The attribute type *emailAddress* MUST NOT be used in DNs. It has been deprecated in RFC 5280, in favour of having an rfc822Name GeneralName in the subjectAltName extension, and recent mail clients can deal with subjectAltName[11,12].

2.3.6 *userID* and *uniqueIdentifier*

The attribute type *userID* or *uid* {0.9.2342.19200300.100.1.1} MUST NOT be used in DNs. The attribute *uniqueIdentifier* {2.5.4.45} MUST NOT be used in DNs. Additionally, it is not relevant for CA certificates of any kind[13].

2.4 Extensions in CA certificates

For operation as a CA certificate, only basicConstraints and keyUsage extensions need to be present in the (root or subordinate) certificate. To be functional as an issuer certificate, there is

[10] *serialNumber* attribute was originally intended to describe the serial number of a device [7]. There have been discussions on the PKIX mailing lists on whether it was also appropriate for persons, and then only to distinguish different persons with the same *commonName* from each other. In particular, it is not intended to contain the certificate serial number.

There is another reason not to use the *serialNumber* attribute: versions of OpenSSL up to and including version 0.9.6 use a non-standard string representation "SN" for this attribute. This representation collides with the recognised abbreviated representation of the *surname* attribute. This representation has changed in OpenSSL 0.9.7 and later to read "serialNumber", so depending on the OpenSSL version used the string representations of DNs with the *serialNumber* RDN attribute type will differ, leading to problems in authorisation.

[11] String representation issues with the *emailAddress* attribute in DNs are caused by OpenSSL, where versions up to and including 0.9.6 used the non-standard string representation "Email" for this attribute type, and later versions use "emailAddress", thus resulting in different string representations for the same DN and leading to problems in subsequent authorisation decisions.

[12] CA certificates themselves are not usually used to sign email, so mail client support is not an issue to be considered for CA certificates.

[13] The string representation of the *userID* or *uid* attribute is not uniquely defined. OpenSSL versions up to and including 0.9.6 have no string representation for this, and this omission has resulted in some versions of the Globus Toolkit that use this OpenSSL version to forcibly re-code the string representation of this attribute to read "USERID". Recent OpenSSL versions stringify it to the RFC 4514 standard representation "uid", resulting in a non-unique representation. Note that both "uid" and "userid" are valid standard string representation of the attribute with OID 0.9.2342.19200300.100.1.1, with "userid" defined in RFC 1274 and "uid" in RFC 4514. The *uniqueIdentifier* attribute, with OID 2.5.4.45, has been string encoded in OpenSSL as "uid", also colliding with the *userID* attribute name.

no *a priori* requirement by (grid) software for any other extensions in the certificate.

Summary of extensions and attribute usage	
Required	basicConstraints, keyUsage, subjectKeyIdentifier, authorityKeyIdentifier
Advised to use	
Optional	for all CAs: cRLDistributionPoints, for subordinate CAs: certificatePolicies, authorityInformationAccess
Should not be used	extendedKeyUsage, nsPolicyURL, nsRevocationURL, nsComment, nsCertType, nameConstraints (for grid-only CAs)

2.4.1 basicConstraints

The basicConstraints extension MUST be included in CA certificates, and it MUST be set to "CA: TRUE". This extension SHOULD be marked as critical[14].

2.4.2 keyUsage

The keyUsage extension MUST be included in CA certificates, and it SHOULD be marked as critical.

For a CA certificate, keyCertSign MUST be set, and crlSign MUST be set if the CA certificate is used to directly sign issued CRLs[15].

It is RECOMMENDED to set no more than these two values[16]. For proper operation it is not required to have more than keyCertSign and cRLSign in the CA certificate and adding additional values may convey an impression to relying parties that the CA certificate is used for purposes other than signing and issuing certificates and related signing services. The CA thus ensures that the permitted use of public keys is minimal and relevant to the goals of its PKI, particularly for its own public key (in the CA certificate)[17].

[14] RFC 5280 states that this extension MUST be marked critical if the certificate is a CA which issues certificates. Some middleware is known not to be able to interpret the basicConstraints extension and CA certificates have been distributed to this effect [8], it may therefore be necessary in some cases to relax the constraint. No grid middleware is known to require this concession.

[15] There may be CAs that either do not issue CRLs at all, since their end-entity certificates have a short lifetime, or that use indirect CRLs. Note that indirect CRLs have not been extensively tested, and are not currently supported by OpenSSL. There is also no direct way to create such an end-entity certificate in some CA products, such as the Sun One/Iplanet CMS, although direct generation of the ASN.1 is always a possibility. Grid middleware currently cannot use indirect CRLs.

[16] If OCSP responses are directly signed by the CA certificate, then digitalSignature MAY be added to the keyUsage extension, since future discussions in the IETF PKIX group may lead to this keyUsage being required to validate the OCSP responses.

[17] A CA can limit permitted use by defining acceptable and unacceptable uses in the policy statements, but

2.4.3 extendedKeyUsage

The extendedKeyUsage extension SHOULD NOT be included in CA certificates[18]. If present, it MUST NOT be marked critical.

2.4.4 nsCertType, nsComment, nsPolicyURL and nsRevocationURL

The ns* extensions are deprecated and MUST NOT be included in any new CA certificates[19].

2.4.5 certificatePolicies

The presence of a certificatePolicies extension is not harmful, but adding this extension in self-signed root CA certificates permanently binds this CA certificate to the particular instance of the policies referenced and is thus not advisable[20]. The certificatePolicies extension MAY be set for subordinate CAs and if set MUST include only policy OIDs.
If present, it SHOULD NOT be marked critical.

2.4.6 cRLDistributionPoints

The cRLDistributionPoints (CDP) extension MAY be present in a self-signed root CA certificate, MUST be included in end-entity certificates, and SHOULD be included in any intermediate CA certificates[21] that issues CRLs.

---

also by setting the appropriate extensions in the certificates. Compliant software will then find it harder to use the CA's public keys for inappropriate purposes. If it is found that the CA's public keys are used for purposes contrary to the defined goals of its PKI, it can adversely affect the CA's name, reputation, or operations, and, ultimately, the most precious thing it has—trust.

[18] extendedKeyUsage should not be included not only because the values of this attribute are not normally relevant for CA certificates, but also it will make the certificate unsuitable for use with Microsoft Internet Explorer up to and including version 6, and unsuitable for use with any version of Microsoft Outlook, as these products will make a logical 'and' between keyUsage and extendedKeyUsage extensions for potentially unrelated usages.

[19] If adding explicit text to the certificate is desired, such as was possible using the nsComment extension, the new attribute to put such text in is the certificatePolicies.userNotice.explicitText (encoded as an IA5String). Note that RFC 5280 RECOMMENDS that only an OID is used in the certificatePolicies extension. Also, compliant RFC 5280 implementations SHOULD actually display each and every user notice to the user.

[20] Any change in the policy requires re-issuing the CA certificate with an updated extension, and re-issuing and re-distributing a CA certificate is a complicated operation. It is therefore advisable to put only long-term stable extensions in a CA certificate.

[21] Client software can use the cRLDistributionPoints extension to retrieve CRLs on-demand, although no known grid software implementations today actually does that.

Note that by putting a CRL distribution URL in any CA certificate the authority implies that the URL will not change during the lifetime of the root or subordinate CA certificate, so, if included here, one SHOULD make sure the URL will be stable over the life time of the certificate.

For a subordinate CA's certificates, where a CDP is present, it MUST contain at least one http URI[22] pointing to a DER formatted CRL for its *issuer*.

2.4.7 authorityKeyIdentifier and subjectKeyIdentifier

A subjectKeyIdentifier extension MUST be included in CA certificates to aid in validation path construction. An authorityKeyIdentifier MUST be included in all CA certificates that are not self-signed[23]. A self-signed root certificate MAY include authorityKeyIdentifier.

An authorityKeyIdentifier extension MUST contain a keyIdentifier with the key identifier ([2], section 4.2.1.1) value of the issuer; in particular, for a self signed root certificate, it MUST have the same value as the subjectKeyIdentifier.

If either of these extensions is included, it SHOULD include only the keyIdentifier option and no other.

2.4.8 subjectAltName and issuerAltName

No stipulation.

2.4.9 authorityInformationAccess

The authorityInformationAccess (AIA) extension for subordinate CAs MAY include OCSP information[24] and issuing CA location.

2.4.10 nameConstraints

The extension nameConstraints (OID {2.5.29.30}) is not relevant for grid purposes today and its use is NOT RECOMMENDED[25].

[22] A CDP should be a HTTP URI; as the CRL is already signed by the issuing CA, using HTTPS adds no extra security and may cause problems. In particular, if the HTTPS endpoint is secured with a certificate from the same CA as the certificate which is being checked, software attempting to fetch a CRL will then check the host certificate validity, for which they need to fetch the CRL, for which they need to check the host certificate validity,... Also, if the CA issuing the host certificate isn't known to the browser, fetching the CRL is also likely to fail.

[23] Not including the subjectKeyIdentifier or authorityKeyIdentifier is not known to break any grid software.

[24] Running an OCSP responder, according to current best practices, is recommended and it should be run as a highly-available service on a 24x7 basis. If such a production OCSP responder is available, its access information SHOULD be included in the AIA extension. If no highly-available OCSP service is present, there SHOULD NOT be an OCSP end-point included in the AIA extension.

[25] The interpretation of the nameConstraints extension varies significantly between implementations and therefore SHOULD be avoided in CA certificates, and is not relevant for end-entity certificates. Note that this applies to CA-defined namespace constraints, and this is completely independent of any constraints on the subject signing

3 End-entity certificates

3.1 General provisions

All end-entity certificates MUST be in X.509 version 3 format, i.e. the version number MUST be set to the value "2", as the use of specific extensions, such as basicConstraints and keyUsage, is required.

3.2 Serial Number

The serial number of each issued certificate MUST be unique amongst all certificates issued by the same issuer DN.

Certificate Serial numbers MUST comply with RFC 5280, section 4.1.2.2. i.e. They MUST be a unique (for all certificates issued by the same CA[26]) positive integer less than 2^{159}.

3.3 Subject distinguished names

The same general considerations mentioned for CA certificate subject names also apply to subject names in end-entity certificates.

Relative Distinguished Name (RDN) attribute types other than "DC", "C", "ST", "L", "O", "OU", and "CN" SHOULD NOT be used.

To ensure uniqueness and proper delegated ownership of the certificate subject namespace, the use of *domainComponent* RDN components corresponding to a duly registered DNS name [11] of the authority at the start of the distinguished name is strongly encouraged. In this case, the ASN.1 SEQUENCE MUST begin with the *domainComponent* attribute corresponding to the top-level domain (e.g. "org", or "eu"), and then be followed by the subordinate domain name components.

The length of the string representation of the subject Distinguished Name (DN) SHOULD[27] limited to no more than 330 characters, in order to allow the URL encoding of the subject DN to be used as a key in a Unix file-system based directory such as the SlashGrid framework[28]

namespace to be defined by the relying party, and which is to be independently enforced by software, such as discussed in GFD.189 [9].

[26] To clarify, RFC 5280's section 4.1.2.2 Serial numbers Uses the term 'CA'. It is only necessary to enforce uniqueness between certificate issued by the same Issuer DN, as Issuer and Serial Number are used together to bind authorisation credentials to the holder of the certificate. see e.g. RFC 5755 [10]

[27] recommendation due to limitations in current implementations

[28] The SlashGrid framework (McNab, 2001) defines a "gridmapdir" mechanism for Unix account provisioning systems such as GridSite and LCMAPS, using a URL-encoded version of the DN as part of a filename. Up to

Subject name RDN components	
Required	*commonName*
Advised to use	*domainComponent*, *organisationName*
Optional	*countryName*, *stateOrProvinceName*, *localityName*, *organisationalUnitName*
MUST NOT be used	*serialNumber*, *emailAddress*, *userID* (also known as 'uid'), *uniqueIdentifier* (also known as 'uid'), *streetAddress*, *postalCode*

3.3.1 *commonName*

A *commonName* attribute MUST be used in the subject DN of an end-entity certificate[29].
If the *commonName* is not encoded as PrintableString, it SHOULD be encoded as UTF8String.

To prevent name collisions between different entities, mainly in issuing personal certificates, a number or other allowed distinguishing characters can be added to the *commonName* to ensure uniqueness[30]. It is allowed for an entity to have more than one subject DN assigned.

For certificates issued to networked entities, typically the (primary) Fully Qualified Domain Name (FQDN) of the server is included in the *commonName*. For regular network entity certificates, there MUST NOT be any additional characters in the *commonName*[31].

Some software[32] contains a legacy feature that allows implicit wildcard matching of the domain name in the *commonName* attribute, where the first component of the domain name containing a dash ("–") is stripped of all characters from the dash onwards, and then matched to the FQDN in the *commonName*[33].

approx. 30 characters are then used for internal purposes. The maximum length of a file name is limited to 1024 characters in the POSIX specification. A URL encoding MAY extend the length of a any string to at most 3 times its byte size, the 330 character indication thus being approx. 990 divided by 3.

[29]Many browsers use only the *commonName* to label certificates in their certificate stores. It should be noted that past versions of the FreeRadius (`http://www.freeradius.org/`http://www.freeradius.org/ [Accessed 2014-06-26]) uses only the *commonName* for its authorisation decision. No grid middleware is known to act in this manner.

[30]Adding qualifiers to the *commonName* is preferred over adding other attributes to the subject DN, such as the uid's or *serialNumber* attributes that MUST NOT be used.

[31]Some components of some grid middleware also recognize Kerberos-style "service" names in the CN as well that look like "servicename/fqdn". In almost all cases a "normal" server certificate without the "servicename/"-qualifier can be used as well—although the documentation of the middleware will not always state that clearly. The "servicename/"-qualifiers SHOULD NOT be used, and they MUST NOT be used wherever compliance with public trust is expected. Use of additional characters in *commonName* is incompatible with the CABForum Baseline Requirements.

[32]This refers in particular to the Globus Toolkit, at least up to and including version 5.

[33]For example: a certificate issued to "CN=grid.example.org" can be used for successfully proving the identity of "grid-ce.example.org" as well as "grid-se.example.org" and "grid.example.org" itself.

Note that for name-based virtual hosting, additional FQDNs can be asserted in the subjectAltName extension in multiple dNSName GeneralNames[34].

3.3.2 *domainComponent*

To ensure subject name uniqueness and proper namespace delegation, the use of *domainComponent* (DC) naming corresponding to a registered DNS name owned by the authority at the beginning of the issuer and subject name RDN sequence is strongly encouraged. In that case, the ASN.1 SEQUENCE MUST start with the domainComponent representing the top-level domain, for example "`DC=org`" or "`DC=eu`".

Since all known software correctly parses all incoming encodings, all of PrintableString, IA5String and UTF8String MAY be used to encode *domainComponent*. IA5String is RECOMMENDED in this case[36] (see section 4.3.2). The value of each *domainComponent* RDN MUST NOT contain characters other than the ACSII characters: `0-9`, `a-z`, `A-Z`, '`-`' (hyphen) and '`_`' (underscore).

3.3.3 *countryName*, *stateOrProvinceName*, *localityName*, *organisationName*, *organisationalUnitName*

If the *countryName* (C) attribute is used, the value of this attribute SHOULD contain the two-letter ISO3166 encoding of the country's name[37,38]. The *countryName*, if used, MUST be used at most once.

Any of the *stateOrProvinceName* (ST), *localityName* (L), *organisationName* (O), and *organisationalUnitName* (OU) attributes MAY be used and SHOULD be used in the intended X.501 sense.

[34] Many browsers modern[35], such as Microsoft Internet Explorer version 6 and higher, or Mozilla Firefox versions 1.5 and higher, will recognize these additional dNSNames in the subjectAltName and recognise it as valid alternate names for the virtual web site.

[36] It is customary to encode the *domainComponent* as an IA5String.The latest OpenSSL and the RedHat Certificate System versions encode the domainComponent attribute as an IA5String, OpenSSL 0.9.7c and older as PrintableString.

[37] The designation UK is an well-known exception, mainly for historical reasons—GB is the official ISO 3166-1 representation for the United Kingdom of Great Britain and Northern Ireland, although in many contexts the designation "UK" is used for the same. Either GB and UK MAY be used as designations. Note that the Ukraine MUST be encoded as UA.

[38] In case the *countryName* (C) is used as part of the varying part of the subject distinguished name (i.e., it is not part of the constant DN prefix that defines the issuing namespace), the *countryName* (C) asserted in the subject DN of an end-entity certificate SHOULD correspond the home country of the end-entity, and thus does not necessarily reflect and is not necessarily the same as the country in which the CA is operating, or the country code in the issuer DN. Therefore, in such cases the *countryName* attribute should not be part of a unique subject DN naming prefix.

The use of at least one descriptive *organisationName* (O) attribute in the DN is RECOMMENDED.

3.3.4 *serialNumber*

The AttributeType *serialNumber* (i.e. {2.5.4.5}) MUST NOT be used in any Name[39].

Specifically, the *serialNumber* attribute MUST NOT be used to re-encode the certificate serial number in the subject name[40].

3.3.5 *emailAddress*

The attribute *pkcs9email* (OID: 1.2.840.113549.1.9.1, "emailAddress") MUST NOT be used in subject DNs[41]. If required, email addresses SHOULD be placed in the subjectAltName extension. Email addresses MUST be encoded in RFC 822 [12] "addr-spec" format (section 6.1) and they MUST be encoded as IA5String.

3.3.6 *userID* and *uniqueIdentifier*

The attribute *userID* (i.e. OID {0.9.2342.19200300.100.1.1}) and *uniqueIdentifier* (i.e. OID {2.5.4.45}) MUST NOT be used in DNs[42]. Both attribute types are also known as "uid".

3.3.7 *streetAddress* and *postalCode*

The attributes *streetAddress* and *postalCode* are either not consistently represented in software, or are not recognised as valid attributes[43]. They MUST NOT[44] be used.

[39] See footnote 10 to section 2.3.4 for clarification.

[40] Not only is such use of *serialNumber* redundant, but it also makes renewals impossible.

[41] The emailAddress attribute in the subject DN has been deprecated in RFC 5280 [2], in favour of having an RCF 822 Email Address [12] in the subjectAltName extension. Many recent mail clients are able to deal with the subjectAltName. Parsing issues with this attribute are caused by OpenSSL, which in versions up to and including 0.9.6 used the non-standard string representation "Email" for this attribute type, whereas other software renders it as "E", or as the numeric OID.

[42] See footnote 13 to section 2.3.6 for clarification.

[43] e.g. Java's X500Principal class rejects PostalCode outright with java.io.IOException: Invalid keyword "POSTALCODE".

[44] recommendation due to limitations in current implementations

3.4 Extensions in end-entity certificates

For use of an end-entity certificate with grid software, at least either of the extendedKeyUsage or nsCertType[45] extensions MUST be present, where the use of the extendedKeyUsage extension is preferred. Including basicConstraints is RECOMMENDED.

End-entity certificates MUST include the keyUsage extension and it is RECOMMENDED that an end-entity certificate also includes the extensions certificatePolicies, and cRLDistributionPoints.

There is no *a priori* requirement by grid software for any other extension in end entity certificates.

End-entity subject extensions and attribute recommendations	
Required	keyUsage, extendedKeyUsage
Advised to use	basicConstraints, cRLDistributionPoints, certificatePolicies, subjectAltName, authorityInformationAccess
Optional	authorityKeyIdentifier, subjectKeyIdentifier, issuerAltName
SHOULD NOT be used	nsCertType

3.4.1 basicConstraints

The basicConstraints extension is RECOMMENDED to be included in end-entity certificates[46]. The pathLenConstraint MUST NOT be present[47].

If the CA software is capable of generating the basicConstraints extension with a cA field even if its value is "CA:FALSE", this extension MUST be included in end-entity certificates, and its value MUST be set to "CA:FALSE".

When present, this extension MUST be marked critical.

3.4.2 keyUsage

The keyUsage extension MUST be included in end-entity certificates, and it MUST be marked critical.

For an end-entity certificate, it depends on certificate usage which values need to be set:

[45] The use of nsCertType is deprecated, see section 3.4.4.

[46] According to the ASN.1 encoding rules, a value "CA:FALSE" for basicConstraints is the default and thus should not need to be encoded as an extension, but discussions leading up to RFC 5280 (`http://www.imc.org/ietf-pkix/old-archive-03/msg00481.html` [Accessed 2014-06-26]) have made clear that it would be strongly advisable to include it.

It is not known if there is client software that will incorrectly allow signing of subordinate certificates if this extension is absent.

[47] Note that RFC 5280 forbids the use of pathLenConstraints in end-entity certificates. If it is included anyway, it would have to allow for an unlimited path length to allow the user to issue proxy certificates [13].

The digitalSignature and keyEncipherment values/bits MUST be set for authentication in SSL sessions, and thus for typical grid usage, as otherwise grid authentication will not work. These two are the only values that are actually required.

The keyAgreement, encipherOnly, and decipherOnly values/bits primarily apply to DH keys, and need not normally be asserted in an end-entity certificate.

The nonRepudiation (contentCommitment) value/bit SHOULD NOT be set for server certificates (including "host" and "service" certificates), as it implies that any use of the key would constitute incontrovertible evidence that the signing was done in a conscious way, which is unlikely for a server certificate. It SHOULD NOT be set in other end-entity certificates either, as the claims made by this keyUsage are ill-defined or non-verifiable, and its interpretation by clients unclear. If it is set regardless, its assertion in personal end-entity certificates SHOULD be limited to special purposes.

The dataEncipherment value/bit is RECOMMENDED in order to enable use of the certificates with specific implementations of message-level security mechanisms where messages are to be encrypted[48].

The keyCertSign and cRLSign values/bits MUST NOT be set in an end-entity certificate, unless the certificate is explicitly intended for use in indirect CRL signing[49].

3.4.3 extendedKeyUsage

The extendedKeyUsage (EKU) extension SHOULD be included in end-entity certificates, but MUST NOT be marked critical.

For personal end-entity certificates or automated entities, clientAuth value/bit SHOULD be asserted in the EKU. But in the grid context, servers at times do act like clients, and thus for host or service certificates it does make sense to include both serverAuth value/bit as well as clientAuth value/bit[50].

OCSP responder certificates MUST have oCSPResponder value/bit asserted.

[48] The dataEncipherment usage is intended to refer to the direct use of the RSA key in enciphering data, and as such ought to bear no relevance to the encryption of documents with a session key, however some web services stacks to date require this usage to be set in order to use the certificate for use in XML encryption and message-level security. This has been verified for exchanging encrypted messages via GSISecureMessage as implemented in the Globus Toolkit middleware. This includes the receiving entity's certificate that must have the dataEncipherment keyUsage extension set if keyUsage itself is set to be a critical extension.

[49] See also section 2.4.2.

[50] This dual-use of host and service certificates action in both a server and a client role is required for, for example, the Network Job Service (NJS) and the Gateway in the Unicore grid middleware, where one NJS may forward a request to another NJS, and in this interaction the NJS acts as a client.

3.4.4 nsCertType, nsComment, nsPolicyURL and nsRevocationURL

nsCertType

This extension is deprecated. It MUST NOT be used in new certificates; the appropriate equivalent values SHOULD be expressed in the extendedKeyUsage extension[51].

nsPolicyURL, nsRevocationURL

These attributes are deprecated and MUST NOT be used in end-entity certificates.

nsComment

This attribute is deprecated and SHOULD NOT be used in end-entity certificates[52]. If it is included, this extension MUST NOT be marked critical.

3.4.5 certificatePolicies

The certificatePolicies extension SHOULD be included and be used in accordance with RFC 5280 (section 4.2.1.4).For an IGTF CA, it is RECOMMENDED to use IGTF OIDs [14] to promote interoperation.

3.4.6 cRLDistributionPoints

The cRLDistributionPoints extensions MUST be present in end-entity certificates, and MUST contain at least one http URI (*i.e.*, not an *https* URI) although it may contain other URIs[53,54,55]. It MUST return the CRL in DER encoded form.

[51] The extendedKeyUsage and nsCertType extensions are interrelated and partially cover the same purposes. Either of these has to be present to ensure correct operation of grid and other software, and nsCertType MUST NOT be used. For example for certificates issued to a Unicore NJS service, the nsCertType can be set to "server, client" but the preferred way to expressing this is by setting eKU to "serverAuth, clientAuth".

[52] If adding explicit text to the certificate, such as was possible using the nsComment extension, is desired, the new attribute to put such text is the certificatePolicies.userNotice.explicitText (encoded as an IA5String). Note that RFC 5280 RECOMMENDS that only an OID is used in the certificatePolicies extension. Also, compliant RFC 5280 implementations SHOULD actually display each and every user notice to the user.

[53] See also footnote 21 to section 2.4.6.

[54] Note that OpenSSL is not able to display the values of the reasons and the cRLIssuer associated with a directoryName or uniformResourceIdentifier.

[55] The cRLDistributionPoints extension should contain (a list of) locations where the actual CRL data is stored, e.g. `URI:http://www.example.org/ca/cacrl.der`. The data retrieved must be the actual CRL. Preferably it returns a direct answer and not a 302 'HTTP redirect', in order to allow caching of the results.

Some software[56] is unable to handle any values other than a single URI in this extension.

It is RECOMMENDED that the reply returned at the http URI is cacheable[57].

3.4.7 authorityKeyIdentifier and subjectKeyIdentifier

subjectKeyIdentifier

The subjectKeyIdentifier (SKI) extension MUST NOT be marked critical.

authorityKeyIdentifier

The authorityKeyIdentifier (AKI) is not usually interpreted by the software, and is considered harmless to current known grid software. The AKI extension MUST NOT be marked critical.

If the AKI in an end-entity certificate contains information that changes when the issuer certificate is modified, it may block a 'smooth' replacement of issuer certificates (e.g. when updating a CA certificate to modify the expiry date). Thus, the authorityCertSerialNumber MUST NOT be used.

Possible other values in AKI include the directoryName of the authority that issued the issuer certificate, which is safe to include as it should not change, or the keyIdentifier of the end-entity issuing CA. If the keyIdentifier has been generated using one of the two recommended methods from RFC 5280 (i.e., is purely derived from the public key value), it will not impair smooth replacement.

3.4.8 subjectAltName and issuerAltName

The subjectAltName extension SHOULD be present for server certificates (including "host" and "service" certificates in the grid context), and, if present, MUST contain at least one FQDN in the dNSName GeneralName. If the certificate contains a CN, then the CN SHOULD consist of *the same FQDN* as one of the subjectAltName dNSName values[58].

If an end-entity certificate needs to contain an rfc822 email address, this address SHOULD be included in the subjectAltName as an rfc822Name GeneralName. The email address MUST NOT form part of the Subject DN (see 3.3.5).

[56] This defect is only known to apply to VOMS and VOMS-Admin, at least up to and including VOMS version 1.7.

[57] The http CRL URL will be downloaded extremely frequently. To allow for web caching of the CRL, it is RECOMMENDED that the web server return a 200 response to the HTTP GET request, and not a 302 redirection, since such an answer it is not normally followed by clients or cached by web caches [15]. It is RECOMMENDED that the CRL be labelled with the correct MIME document type.

[58] If the certificate contains more than one CN, then one of them should be the same as the subjectAltName.

Multiple FQDNs, in host certificates, MAY be added as dNSName GeneralNames[59]. Every name that clients will use to connect to the server(s) SHOULD be contained in the subjectAltName extension, cf. RFC2818, section 3.1 (server identity). There is no need to include the canonical name if it is different from the name the clients use.

Wildcards in hostnames SHOULD NOT be used (they are not FQDNs); if used, the SHOULD be a single '*' used as, and only as, the most specific (leftmost) entry in the domain name (cf. [16], 3.1), *e.g.*, '`*.example.com`'.

3.4.9 authorityInformationAccess

The authorityInformationAccess extension is used by the issuer to refer the validator to an OCSP service that the issuer recommends using.

It is RECOMMENDED to include this extension if the issuer operates a production-quality OCSP service. The extension SHOULD NOT be included unless it points to a highly-available service.

The extension MAY also contain a CRL URI, as described in RFC 4325, or the location of any higher-level CA certificates, but it should be noted that regardless, a CRL http URI MUST also be included in the cRLDistributionPoints extension.

The extension MUST NOT be marked critical.

3.4.10 nameConstraints

No additional stipulation.

4 General Considerations

4.1 Message Digest Algorithms

For the message digest that protects the certificate integrity, known-weak signatures or hash functions, such as MD5 (RFC 1321 [17]) and SHA-1 (RFC 3174 [18]), MUST NOT be used in new certificates (RFC 6151 [19]), since the MD5 hash function known to have collisions, and SHA-1 has been shown to provide less than 80 bits of security. The current most secure hash function that is supported by the entire target audience of the CA SHOULD be used. In particular SHA-2 (RFC 6234 [20]) SHOULD be used and a digest function at least as strong as SHA-256

[59] An example is a web server certificate where the server supports hosting of several secured web sites.

MUST be used[60].

4.2 ASN.1 Structure of the DN and ordering of the RDN components

The subject and issuer distinguished Names (DNs) consist of a sequence (an order-preserving list) of Relative DN (RDN) components sets. As stated in the preceding sections, the length of any RDN set MUST be equal to one (1).

There has, however, not been definitive guidance on the way the RDN components should be ordered in the DN sequence, neither from the X.500 document series (specifically X.521 [21]), nor from sources such as the X.509 Style Guide [22]. The definition of the Name in X.501 [23] defines it as a SEQUENCE OF RelativeDistinguishedNames, where the SEQUENCE OF is an ASN.1 construct that in the DER encoding should be written out "as-is" in the order in which it is presented. It should not be re-ordered for interpretation[61].

```
Name ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeValueAssertion
AttributeValueAssertion ::= SEQUENCE {
    attributeType OBJECT IDENTIFIER,
    attributeValue ANY
}
```

Since many authorisation applications and namespace constraining policies are based on string wildcard matching of only the trailing part of an OpenSSL one-line string representation of the Name, the SEQUENCE of RelativeDistinguishedNames SHOULD start with the least-varying component (i.e. the static prefix) of the distinguishedName for all issuer and subject names, and MUST start with the least-varying component for any names issued by an authority that issues either end-entity certificates, or issues certificates to three or more subordinate authorities[62].

[60] If compatibility with versions of Microsoft Windows before April 2015 is required, SHA-512 SHOULD NOT be used due to compatibility issues with its TLS 1.2 implementations; see Microsoft Knowledge Base article 2973337 for details.

[61] This ordering applies for comparisons based on the ASN.1 structure. The representation of that ASN.1 SEQUENCE as a string is subject to many discussions and conflicting solutions, as is testified to by the long debates regarding the representation returned by the OpenSSL X509_one_line function and the string representation defined in RFC 4514.

[62] Discussions around RFC 5280 have included statements that the SEQUENCE ought to start with the Country or a *domainComponent*. Formerly, it could only be deduced from the examples, and the unclear guidance "In theory it should be a full, proper DN, which traces a path through the X.500 DIT", which usually interpreted "trace" as "start at the root of the tree".

4.3 String encoding of the RDN components

All Relative Distinguished Name (RDN) components in distinguished names MUST be compliant with RFC 5280 [2] and in addition SHOULD be encoded as PrintableString (Section 4.3.1) with the exception of *domainComponent* (Section 2.3.2 & 3.3.2) which SHOULD use IA5String (Section 4.3.2). If a UTF8String is used for encoding, the RDN MUST NOT contain characters that cannot be expressed in printable 7-bit ASCII, as these characters have inconsistent representations[63].

4.3.1 PrintableString encoding

RFC 2252 defines PrintableString as consisting of 'a'–'z', 'A'–'Z', '0'–'9', and the characters '"', '(', ')', '+', ',', '-', '.', '/', ':', '?', ' '.

Summary of PrintableString Characters and encodings		
character(s)	**name**	**Equivalent Unicode name and code point** [24]
'a'–'z',	Latin alphanumeric	LATIN SMALL LETTER A (U+0061) – LATIN SMALL LETTER Z (U+007A)
'A'–'Z',		LATIN CAPITAL LETTER A (U+0041) – LATIN CAPITAL LETTER Z (U+005A)
'0'–'9',		DIGIT ZERO (U+0030) – DIGIT NINE (U+0039)
'"'	double quote	QUOTATION MARK (U+0022)
'(', ')'	left and right parentheses	LEFT PARENTHESIS (U+0028), RIGHT PARENTHESIS(U+0029)
'+'	plus	PLUS SIGN (U+002B)
','	comma	COMMA (U+002C)
'-'	minus/hyphen	HYPHEN-MINUS (U+002D)
'.'	dot/period	FULL STOP (U+002E)
'/'	forward slash[64]	SOLIDUS (U+002F)
':'	colon	COLON (U+003A)
'?'	question mark	QUESTION MARK (U+003F)
' '	space	SPACE (U+0020)

[63] Non-7-bit ASCII characters have different string representations in different pieces of software, and cannot easily be passed around between locales, or be read from log files. Use of such characters will result in undefined or inconsistent behaviour, e.g. in subsequent authorisation. Often, only the string representation is available, e.g. in a log file, and for security reasons such as incident response it should be possible to type the DN from a printed or aural representation of it.

[64] OpenSSL uses forward slash ("/") in the one-line string representation to separate RDNs, making the use of the forward slash potentially confusing. But since there is always an equal sign (=) after the name of a RDN

This set is almost consistent with the PrintableString definition of RFC 1778, differing only in allowing ''' single quote {APOSTROPHE (U+0027)}, instead of '"' double quote {QUOTATION MARK (U+0022)}.

Use of PrintableStrings in RDN Components

The double quote MUST NOT be used.

The single quote SHOULD NOT be used[65]. The colon (":") SHOULD NOT be used[66].

The CA MUST ensure that case or consecutive spaces are not used to distinguish between users (e.g. users with the same name)[67].

4.3.2 IA5String

IA5Strings are strings consisting entirely of 8-bit representation of characters from the ASCII [25] 7-bit character set—defined as the International Alphabet No.5, now known as the International Reference Alphabet (IRA) [26].

4.3.3 UTF8String

For the purposes of this document, a UTF8String consists of a subset of the character set defined in ISO/IEC 10646 [27], with the following provisions:

(a) A UTF-8 encoded string MUST NOT contain non-printable characters (ASCII 31 and below, or ASCII 127).

(b) Character codes where the character representation is subject to national or regional variations SHOULD NOT be used.

(c) In particular, diacritical marks and other combining marks MUST NOT be used.

(d) For security reasons, an implementation SHOULD check for illegal characters and illegal UTF-8.

component in this representation and the equal sign is not part of the allowed character set, a proper parser should be able to parse this correctly.

[65] OpenSSL follows RFC 1778's definition of PrintableString.

[66] The COLON (":") character is used as a field separator in 'htpasswd' files with FakeBasicAuth as used in Apache mod_ssl and cannot be escaped in that format. Subjects with a colon in their DN will not be listable in this file format.

[67] While PrintableString encodings are supposed to be case insensitive [2], in practice most grid software uses case sensitive comparisons. A related problem is found with consecutive spaces which are supposed to be collapsed to a single space.

(e) COLON (':') SHOULD NOT be used (see 4.3.1).

The characters are encoded in UTF-8 according to RFC 3629 [28]. In particular, every character is encoded in one octet.

4.4 Keys and key lengths

As documented in NIST special publication 800-57 [29], 1024-bit RSA keys are considered equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys [30]. RSA claimed that 1024-bit keys were likely to become crackable between 2006 and 2010 and that 2048-bit keys are sufficient until 2030. An RSA key length of 3072 bits should be used if security is required beyond 2030. NIST key management guidelines further suggest that 15360-bit RSA keys are equivalent in strength to 256-bit symmetric keys [68]. As other digital signature and key exchange algorithms are introduced, such as elliptic curve mechanisms, their use should be considered for new certificates provided the entire target audience is capable of dealing with such mechanisms[69].

4.5 Maximum key lengths

As of this writing, RSA keys longer than 8192 bits have not been evaluated in production deployments across all infrastructures supported by IGTF. Elliptic curve keys have not been evaluated in these environments either.

5 Directory Names and String Representations

Although comprehensive texts on the creation of certificate authorities and the configuration of particular CA software exist[70], it is considered appropriate to repeat some of this information here. In particular, the ordering of Relative Distinguished Name (RDN) components in a Directory Name and the string representation thereof remains a source of frequent mistakes. An example of the relation between the ASN.1 DN and its various string representations is given below. This section does not contain normative text.

A typical issuer distinguished name that is compliant to the guidelines given in this document could be:

[68] See also `http://www.keylength.com` [Accessed 2014-01-19] for a comprehensive overview.

[69] At of time of writing, only RSA algorithms are sufficiently well supported in clients. It is thus not advised to select non-RSA algorithms.

[70] See for instance: Aufbau und Betrieb einer Zertifizierungsinstantz, DFN Bericht 79, and especially Chapter 8, `http://www.dfn-cert.de/dfn/berichte/db089/` [Accessed 2014-01-19].

For expressing these in OpenSSL, e.g., `http://www.math.ias.edu/doc/openssl-0.9.7a/openssl.txt` [Accessed 2008-04-03]

RFC 4514 string representation	`CN=My Authority 1, O=MyOrg Authorities, DC=example, DC=org`
OpenSSL oneline representation	`/DC=org/DC=example/O=MyOrg Authorities/CN=My Authority 1`

ASN.1 sequence	`SEQUENCE`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :domainComponent`
	`  IA5STRING :org`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :domainComponent`
	`  IA5STRING :example`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :organization`
	`  PRINTABLESTRING :MyOrg Authorities`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :commonName`
	`  PRINTABLESTRING :My Authority 1`

RFC 4514 string representation	`CN=My Authority 1, O=MyOrg Authorities, C=lu`
OpenSSL oneline representation	`/C=lu/O=MyOrg Authorities/CN=My Authority 1`

ASN.1 sequence	`SEQUENCE`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :country`
	`  PRINTABLESTRING :lu`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :organization`
	`  PRINTABLESTRING :MyOrg Authorities`
	`  SET`
	`  SEQUENCE`
	`  OBJECT :commonName`
	`  PRINTABLESTRING :My Authority 1`

While for an end-entity names "Jürgen Schmidt", the following forms could be used:

RFC 4514 string representation	CN=Juergen Schmidt 90210, DC=example, DC=org
OpenSSL oneline representation	/DC=org/DC=example/CN=Juergen Schmidt 90210

ASN.1 sequence	SEQUENCE
	  SET
	  SEQUENCE
	  OBJECT :domainComponent
	  IA5STRING :org
	  SET
	  SEQUENCE
	  OBJECT :domainComponent
	  IA5STRING :example
	  SET
	  SEQUENCE
	  OBJECT :commonName
	  PRINTABLESTRING :Juergen Schmidt 90210

RFC 4514 string representation	CN=Juergen Schmidt 90210, O=ExOrg B.V., C=nl
OpenSSL oneline representation	/C=nl/O=ExOrg B.V./CN=Juergen Schmidt 90210

ASN.1 sequence	SEQUENCE
	  SET
	  SEQUENCE
	  OBJECT :country
	  PRINTABLESTRING :nl
	  SET
	  SEQUENCE
	  OBJECT :organization
	  PRINTABLESTRING :ExOrg B.V.
	  SET
	  SEQUENCE
	  OBJECT :commonName
	  PRINTABLESTRING :Juergen Schmidt 90210

6 Security Considerations

The correct and complete interpretation of any and all parts of a certificate is essential to maintain integrity of the system that relies on them. Inconsistencies in name ordering and representation, as well as the use of non-standard attributes and extensions that are not well tested with the validation software and subsequent authorisation systems may leave holes in a deployment which relies upon X.509 certificates. Where such adverse interactions are known, they have been highlighted in the corresponding sections of this document. However, the absence of any such

warnings may not be construed as to mean that no security issues exist.

7 Contributors

This document captures the collective knowledge of many people, and the editors are grateful for the essential contributions made to this document by the members of the International Grid Trust Federation (IGTF, see http://www.gridpma.org/), the individual certification authorities and their staff, and relying parties that have conducted the experiments and tests, and the contributions from the participants in the CAOPS WG.

David L. Groep (Editor)
Nikhef, Dutch National Institute for Sub-atomic Physics,PDP/Grid group
Room: H1.50, PObox 41882, NL-1009DB
Amsterdam
The Netherlands
Email: davidg@nikhef.nl

Michael A. S. Jones (Editor)
Jisc
6th Floor, Churchgate House
56 Oxford Street
Oxford Road, Manchester
United Kingdom
Email: mike.jones@jisc.ac.uk

Jens Jensen (Editor)
Scientific Computing Department
R89, F22
STFC Rutherford Appleton Laboratory
Harwell Oxford Campus
Chilton
Didcot
Oxfordshire, OX11 0QX
Email: jens.jensen@stfc.ac.uk

8 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.

9 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.

10 Full Copyright Notice

11 References

[1] David L. Groep, Michael Helm, Jens Jensen, Milan Sova, Scott Rea, Reimer Karlsen-Masur, Ursula Epting, and Mike Jones. Grid Certificate Profile. GFD-C.125, March 2008.

[2] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2008. URL http://www.ietf.org/rfc/rfc5280.txt. Updated by RFC 6818.

[3] International Telecommunication Union. The directory: Public-key and attribute certificate frameworks. ITU-T Recommendation X.509, November 2008. URL http://www.itu.int/rec/T-REC-X.509.

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

[5] R. Housley and S. Santesson. Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 4630 (Proposed Standard), 2006. URL http://www.ietf.org/rfc/rfc4630.txt. Obsoleted by RFC 5280.

[6] ISO (International Standards Organization) 3166 Maintenance Agency. Country Codes - ISO 3166. URL http://www.iso.org/iso/country_codes.htm.

[7] International Telecommunication Union. The directory: Selected attribute types. ITU-T Recommendation X.520, November 2008. URL http://www.itu.int/rec/T-REC-X.520.

[8] Vivek Kaushik. Digital Certificate Extensions: Should "Basic Constraints" Be Marked Critical?, September 2007. URL http://www.netrust.net/BasicConstraints_whitepaper_v1.0.pdf.

[9] David L. Groep and Jens Jensen (eds.). Relying Party Defined Namespace Constraints Policies in a Policy Bridge PKI Environment. GFD.189, June 2011. URL http://www.ogf.org/documents/GFD.189.pdf.

[10] S. Farrell, R. Housley, and S. Turner. An Internet Attribute Certificate Profile for Authorization. RFC 5755 (Proposed Standard), January 2010. URL http://www.ietf.org/rfc/rfc5755.txt.

[11] J. Postel. Domain Name System Structure and Delegation. RFC 1591 (Informational), March 1994. URL http://www.ietf.org/rfc/rfc1591.txt.

[12] D. Crocker. STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES. RFC 822 (INTERNET STANDARD), August 1982. URL http://www.ietf.org/rfc/rfc822.txt. Obsoleted by RFC 2822, updated by RFCs 1123, 2156, 1327, 1138, 1148.

[13] S. Tuecke, V. Welch, D. Engert, L. Pearlman, and M. Thompson. Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. RFC 3820 (Proposed Standard), 2004. URL http://www.ietf.org/rfc/rfc3820.txt.

[14] Interoperable Global Trust Federation. URL https://www.eugridpma.org/objectid/.

[15] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616 (Draft Standard), 1999. URL http://www.ietf.org/rfc/rfc2616.txt. Updated by RFCs 2817, 5785, 6266, 6585.

[16] P. Mockapetris. Domain names - concepts and facilities.

[17] R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321 (Informational), April 1992. URL http://www.ietf.org/rfc/rfc1321.txt. Updated by RFC 6151.

[18] D. Eastlake 3rd and P. Jones. US Secure Hash Algorithm 1 (SHA1). RFC 3174 (Informational), September 2001. URL http://www.ietf.org/rfc/rfc3174.txt. Updated by RFCs 4634, 6234.

[19] S. Turner and L. Chen. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. RFC 6151 (Informational), March 2011. URL http://www.ietf.org/rfc/rfc6151.txt.

[20] D. Eastlake 3rd and T. Hansen. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234 (Informational), May 2011. URL http://www.ietf.org/rfc/rfc6234.txt.

[21] International Telecommunication Union. The directory: Selected object classes. ITU-T Recommendation X.521, November 2008. URL http://www.itu.int/rec/T-REC-X.521.

[22] Peter Gutmann. X.509 style guide, October 2000. URL http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt. visited on 2007-10.

[23] International Telecommunication Union. The directory: Models. ITU-T Recommendation X.501, November 2008. URL http://www.itu.int/rec/T-REC-X.501.

[24] The Unicode Consortium. The Unicode standard, version 6.3.0, 2013. URL http://www.unicode.org/versions/Unicode6.3.0/. visited on 2014-06-30.

[25] U.S. Department of Commerce. Code for information interchange. Federal Information Processing Standards Publication (FIPS PUB) 1, November 1968.

[26] International Telecommunication Union. International reference alphabet (ira) (formerly international alphabet no. 5 or ia5)—information technology—7–bit coded character set for information interchange. ITU-T Recommendation T.50, November 1992. URL http://www.itu.int/rec/T-REC-T.50.

[27] ISO 10646. Information technology – Universal Coded Character Set (UCS), 2012. URL http://standards.iso.org/ittf/PubliclyAvailableStandards/c056921_ISO_IEC_10646_2012.zip.

[28] F. Yergeau. UTF-8, a transformation format of ISO 10646. RFC 3629 (INTERNET STANDARD), November 2003. URL http://www.ietf.org/rfc/rfc3629.txt.

[29] Burt Kaliski. Twirl and rsa key sizes, May 2003. URL http://www.rsasecurity.com/rsalabs/node.asp?id=2004. visited on 2007-10.

[30] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. NIST SP800-57: Recommendation for Key Management Part 1: General(Revised). Technical report, 2007. URL http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf.