GWD-R.125bis DRAFT
CAOPS-WG
davidg@nikhef.nl,
mike.jones@manchester.ac.uk

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

June 2013

Grid Certificate Profile

Todo list

Status of This Document

This document provides **recommendations** to the Grid community. Distribution is unlimited.

We have Distribution is unlimited here and under the copyright heading.

Shouldn't this section contain one of the following statements: Group Working Draft (GWD); Grid Final Draft (GFD); Grid Recommendation; Obsolete. This document is replaced by/obsoleted by GFD-I.xxx; Historical

Obsoletes

This document obsoletes GFD-C.125.

Missing? Document Change History section containing e.g. Updated to conform to GFD-C.152 and cite gfd152.

Add citation mark: gfd125

Copyright Notice

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 grid infrastructures today. The intended audience for this document includes issuers of X.509 certificates for use in grid infrastructures, and implementers of X.509 validation software for grid purposes.

Interoperability for X.509 identity certificates between the issuers of certificates and the software that interprets them is increasingly more important as the number of participants in grids 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 to ensure 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 and the X.509 standard.

This document extends the guidance in GFD.125 by specifying additional constraints and providing further clarification.

Document should refer either to GFD.125 or GFD-C.125 consistently.

Contents

1 Scope of this document

This document provides guidance for the use of attributes and extensions in X.509 [9] certificates such that they are usable by the majority of the grid infrastructures today. This guidance must be interpreted in the context of RFC 5280 [3], *i.e.*, all certificates must be compliant to RFC 5280 in addition to any limitations imposed by the guidelines in this document.

Specific attention has been given to the representation of the subject and issuer distinguished names as strings, since in much of the grid software 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.

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 [2].

2 Self-signed and subordinate Certification Authority certificates

basicConstraints and keyUsage are extensions and should be normaltext?

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.

CheckOK: Removed "in use," from "such as OpenSSL in use,version 0.9.8 and above"

For the message digest that protects the certificate integrity, known-weak signatures or hash functions, such as MD5, MUST NOT be used in new certificates. The current most secure hash function that is supported by the entire target audience of the CA SHOULD be used. In particular SHA-2 or better SHOULD be used and at least as strong as SHA-1 MUST be used[1].

2.2 Serial Number

converted the space n-dash space ' – ' comments to English m-dashes '—'

NB Didn't we agree that extensions were not to be italicsised only attributes.

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

Is this serial number or *serialNumber*?

authorityKeyIdentifier is in italics – we agreed that only attributes and latin was to be italicised IIRC

[1] Note that modern hashes, such as SHA-256, are supported in recent versions of the majority of software (such as OpenSSL version 0.9.8 and above) so SHA-1 is no longer the only available value at the time of writing.

[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 till 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+ that is advised.

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 of the CA certificate. Note that including the attribute serial number in *authorityKeyIdentifier* extension in end-entity certificate is discouraged.

2.3 Issuer and Subject names

Only a limited number of attribute types are well supported by all of the current 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). Use of 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, the ASN.1 SEQUENCE MUST only contain ASN.1 SETs of length 1. Other SET lengths MUST NOT be used.

Suggest "guidance given in X.521"

Contrary to what may be deduced from the guidance given from 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 deployments today 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 multiple *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 much of the known grid middleware uses the entire DN for subject identification. If no O or OU attributes appear in the DN, browsers[3] might not use other components to show affiliation.

All Relative Distinguished Name (RDN) components in distinguished names MUST be compliant with RFC 4630 [6] and in addition SHOULD be encoded as PrintableString. If an 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.

Should be "If a UTF8String

Should the following attributes be in italic?

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

Country Locality capitals also highlighted in v06a?

Issuer and authority subject name RDN component recommendations	
Required	*commonName*
Advised to use	*domainComponent*, *organisationName*
Optional	*countryName*, *stateOrProvinceName*, *localityName*, *organisationalUnitName*
Should not be used	*serialNumber*, *userID*, *uniqueIdentifier*, *emailAddress*

2.3.1 *commonName*

Added italics to common name below

The *countryName* 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 distinguishing the authority's name[4]. In addition the use of the "O" entry is encouraged.

2.3.2 *domainComponent*, *countryName*, *organisationName*, *organisationalUnitName*

Should have and in title

Should be consistant with other headings (either include abreviations here or exclude them later)

Should the paragraph not be earlier in the document?

The distinguished name is usually made up of a combination of the attribute types "DC", "C", "ST", "L", "O", "OU" and "CN".

To ensure uniqueness and proper 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".

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

should be "(O)"

If a *countryName* (C) component is included in the issuer DN, it SHOULD reflect the country in which the issuer is based.

[4]Having a *countryName* 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.

2.3.3 *serialNumber*

The attribute type *serialNumber* {2.5.4.5} MUST NOT be used in any Name[5].

changed "+" to "and later" in footnote

2.3.4 *emailAddress*

The attribute type *emailAddress* MUST NOT be used in DNs. It has been deprecated in RFC 5280, in favour of having an *rfc822EmailAddress*

should be "in favour of the string rfc822Name=*emailAddress*"

in the subjectAltName X.509v3 extension, and many recent mail clients can deal with subjectAltName .[6]

Check Me: Chnaged from subjectAlternativeName

In all cases, the CA certificate itself is not usually used to send email, so mail client support is not an issue to be considered for CA certificates.

SAN also changed

2.3.5 *userID* or *uid*

The attribute type *userID* or *uid* {0.9.2342.19200300.100.1.1} MUST NOT be used in Names. The attribute *uniqueIdentifier* {2.5.4.45} MUST NOT be used in Names. Additionally, it is not relevant for CA certificates of any kind.[7]

should be "sign emails"

[5]The serialNumber attribute was originally intended to describe the serial number of a device [10]. 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 authorization.

[6]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.

[7]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 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.

2.4 Extensions in CA certificates

Again: Extensions here have been marked up in italics for attributes

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

Should the following attributes be in italic

Should extensions AKI and SKI, start with a capital

Summary of extensions and attribute usage	
Required	basicConstraints, keyUsage
Advised to use	AuthorityKeyIdentifier, SubjectKeyIdentifier
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[8].

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[9].

Check if these extensions shoul be in italics

extension italics again?

[8] While the criticality is intended for a CA to make the use of its certificates more robust, not all verification systems currently in use (specifically those outside of the grid context proper) do not factor the criticality of many of these extensions. Especially for CAs that serve a wider community, marking basicConstraints as critical may break other applications, which is the reason it is not marked as such in a sizeable fraction of the CA certificates preinstalled in browsers (as of September 2007, the root store in Microsoft Windows XP contained 85 out of 200 CAs that were not compliant [13]). For new CAs that do not face known incompatibilities, it is strongly recommended to set basicConstraints and mark it critical.

[9] There may be CAs that either do not issue CRLs at all, since their end-entity certificates have a short

It is RECOMMENDED to set no more than these two values[10]. 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)[11].

DigitalSign should be italics

Check: m-dash changed before trust

2.4.3 extendedKeyUsage

The *extendedKeyUsage* extension SHOULD NOT be included in CA certificates[12]. If present, it MUST NOT be marked critical.

2.4.4 authorityInfoAccess

The *authorityInfoAccess* (AIA) extension for subordinate CAs MAY include OCSP information[13] and issuing CA location. nsCertType, nsComment, nsPolicyURL, nsRevocationURL. The *ns** attributes are deprecated and MUST NOT be included in any new CA certificates.[14]

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.

[10] 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.

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

[12] *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.

[13] 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.

[14] If adding explicit text to the certificate is desired, such as was possible using the nsComment extension, 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.

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[15]. 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, but MUST be included in end-entity certificates and SHOULD be included in any intermediate CA certificates[16] that issues CRLs.

For subordinate CAs, where a CDP is present, it MUST contain at least one http URI[17].

2.4.7 *Authority and Subject Key Identifier*

A *subjectKeyIdentifier* extension MUST be included in CA certificates to aid in validation path construction. An *authorityKeyIdentifier* MUST be included in all CA certificates unless the certificate is self-signed[18]. If included for a self-signed root certificate the *authorityKeyIdentifier*'s *subjectKeyIdentifier* and *subjectKeyIdentifier* MUST be the same.

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

[15] 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.

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

[17] The URI should be plain *http*, and in particular not an https. Although the https connection in theory does not need to be validated, many client tools do this by default and will fail in absence of proper certificate, especially if the web site is not secured with a certificate issued by the CA itself. The CRL returned is signed and integrity protected anyway. The *cRLDistributionPoints* extension MAY contain other URIs.

[18] Not including the subject- or *authorityKeyIdentifier* is not known to break any grid software.

2.4.8 nameConstraints

The extension *nameConstraints* (OID 2.5.29.30) is not relevant for grid purposes today and its use is NOT RECOMMENDED[19].

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.

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

For the message digest that protects the certificate integrity, known-weak signatures or hash functions (such as MD5) MUST NOT be used in new certificates. Note that modern hashes, such as SHA-256, are supported by the majority of OpenSSL versions in use, so SHA-2 is currently RECOMMENDED if the software in the entire community supports it. At least a SHA-1 hash or stronger MUST be used.

3.2 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 name space, the use of *domainComponent* RDN components corresponding to a duly registered DNS name citerfc1591 of the authority at the start of the distinguished name is strongly encouraged. Thus, 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.

[19]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 namespace to be defined by the relying party, and which is to be independently enforced by software (for example via 'dot-signing_policy' files in the Globus Toolkit software).

3.2.1 String encoding of the RDN components

All Relative Distinguished Name (RDN) components in distinguished names MUST be compliant with RFC 4630 [6] and in addition SHOULD be encoded as PrintableString. If an 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[20].

3.2.2 PrintableString encoding

RFC 2252 defines PrintableString as consisting of 'a'–'z', 'A'–'Z', '0'–'9', and the characters '"', '(', ')', '+', ',', '-', '.', '/', ':', '?', ' ', that is, upper and lower case alphanumeric, double quote, left and right parentheses, plus, comma, minus/hyphen, dot (period), forward slash[21], colon, question mark, and space. This set is almost consistent with the PrintableString definition of RFC 1778, differing only in allowing ''' (single quote), instead of '"' (double quote).

The double quote MUST NOT be used.

The single quote SHOULD NOT be used[22]. The colon (":") SHOULD NOT be used[23].

The CA MUST ensure that case or consecutive spaces are not used to distinguish between users (e.g. users with the same name)[24].

[20] 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 authorization.

[21] 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 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.

[22] OpenSSL follows RFC1778's definition of PrintableString.

[23] The COLON (":") character is used as a field separator in 'htpassword' 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.

[24] While printableString encodings are supposed to be case insensitive [7], 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.

Subject name RDN components	
Required	commonName
Advised to use	domainComponent, organizationName
Optional	Country, stateOrProvinceName, Locality, organizationalUnit-Name
Should not be used	serialNumber, emailAddress, userID (also known as 'uid'), uniqueIdentifier (also known as 'uid')

Should these attributes be in italic?

3.2.3 *commonName*

A commonName attribute MUST be used in the subject DN of an end-entity certificate[25]. If the *commonName* is not encoded as printableString, it SHOULD be encoded as UTF8String.

Country, Locality, should be capitalised?

To prevent name collisions between different entities, mainly in issuing personal certificates, a number or other allowed distinguishing characters can be added to the CN to ensure uniqueness[26]. It is usually allowed for an entity to have more than one subject DN assigned.

serialNumb attribute italics?

For certificates issued to networked entities, typically the (primary) FQDN of the server is included in the commonName. For regular network entity certificates, there MUST NOT be any additional characters in the commonName[27].

Some grid middleware[28] contains a design flaw that allows implicit wildcard matching of the domainname in the commonName attribute, where the first component of the domainname containing a dash ("-") is stripped of all characters from the dash onwards, and then matched to the FQDN in the commonName[29].

Attribute Name or extenstion.

Note that for name-based virtual hosting, additional FQDNs can be asserted in the *subjectAlternativeName* extension in multiple *dNSName* attributes[30].

[25] 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/) uses only the *commonName* for its authorization decision. No grid middleware is known to act in this manner.

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

[27] Some components of some grid middleware also recognize Kerberos-style "service" names in the CN as well that look like "servicename/fqdn". In the majority of the 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. It is recommended to phase out the "servicename/"-qualifiers where possible.

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

[29] 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.

[30] Many modern browsers, such as Microsoft Internet Explorer version 6 and higher, or Mozilla Firefox versions 1.5 and higher, will recognize these additional *dNSNames* in the *subjectAlternativeName* and recognise

Capitalizati of C and L.

3.2.4 *domainComponent* (DC), *country* (C), *stateOrProvinceName* (ST), *Locality* (L), *organizationName* (O), and *organizationalUnitName* (OU)

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".

It is customary to encode the *domainComponent* as an IA5String[31]. Since all known software correctly parses all incoming encodings, all of PrintableString, IA5String and UTF8String MAY be used to encode *domainComponent*, with IA5String being preferred, and the characters `0-9`, `a-z`, `A-Z`, '`-`' (hyphen) and '_' (underscore) allowed.

If the Country attribute is used, the value of this attribute SHOULD contain the two-letter ISO3166 encoding of the country's name[32], [33]. The country, if used, MUST be used at most once. Any of the *stateOrProvinceName* (ST), *Locality* (L), *organizationName* (O), and *organizationalUnitName* (OU) attributes MAY be used and have their usual meaning.

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

sort labels out

it as valid alternate names for the virtual web site.

[31] The latest OpenSSL and the RedHat Certificate System versions encode the domainComponent attribute as an IA5String, OpenSSL 0.9.7c and older as PrintableString.

Since PrintableString is really a subset of IA5String, one could modify incoming requests with a PrintableString encoding such that IA5String encodings are used in the issued certificates.

[32] 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. Both GB and UK MAY be used as designations. Note that the Ukraine MUST be encoded as UA.

[33] In case the country (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 country (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 *Country* attribute should not be part of a unique subject DN naming prefix.

3.2.5 *serialNumber*

The AttributeType "serialNumber" (i.e. 2.5.4.5) MUST NOT be used in any Name[34].

Specifically, the serialNumber attribute MUST NOT be used to re-encode the certificate serial number in the subject name[35].

following section needs work

3.2.6 *emailAddress*

The attribute *pkcs9email* ("emailAddress") MUST NOT be used in subject names[36]. If used, by RFC 5280 email addresses MUST be encoded in RFC 822 "addr-spec" format (section 6.1) and they MUST be encoded as IA5String.

fix labels ref to section 6.1

3.2.7 *userID* and *uniqueIdentifier*

The attribute type "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 Names[37]. Both attribute types are also known as *uid*.

consistancy in Attribute quote and italics

3.3 Extensions in end-entity certificates

For use of an end-entity certificate with grid software, at least either of the *extendedKeyUsage* or *nsCertType*[38] extensions MUST be present, where the use of the *extendedKeyUsage* extension is preferred. Including *basicConstraints* is RECOMMENDED.

For end-entity certificates issued to networked entities (servers or services), the use of the *subjectAlternativeName* extensions with a *dNSName* attribute is RECOMMENDED. For end-entity certificates that include an rfc822 email address, the *subjectAltName* extension SHOULD be used, and the email address included in the *rfc822Name* attribute.

fix labels footnote 7 and 2.3.5

[34] See footnote 5 to section 2.3.3 for clarification.

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

[36] The emailAddress attribute in the subject DN has been deprecated in RFC5280 [3], in favour of having an *rfc822EmailAddress* in the *subjectAlternativeName* extension. Many recent mail clients are able to deal with the *subjectAlternativeName*. 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.

[37] See footnote 7 to section 2.3.5 for clarification.

[38] The use of nsCertType is deprecated, see section 3.3.5.

get section label in footnote

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, subjectAlternativeName*, authorityInfoAccess
Optional	authorityKeyIdentifier, subjectKeyIdentifier, issuerAlternativeName
Should not be used	nsCertType

Should these attributes be in italic?

3.3.1 *basicConstraints*

The *basicConstraints* extension is RECOMMENDED to be included in end-entity certificates[39]. The *pathLenConstraint* attribute MUST NOT be present[40].

Country, Locality, should be capitalised?

If the CA software is capable of generating the basicConstraints extension with a *cA*attribute 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.

3.3.2 *keyUsage*

Why is there an asterix?

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

RFC3280bis need updating

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

The *digitalSignature* and *keyEncipherment* values MUST be set for authentication in SSL sessions, and thus for typical grid usage, as otherwise grid authentication will not work.

CA

[39]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 recent discussion (on RFC3280bis) has 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.

[40]Note that RFC 5280 forbids the use of pathLenConstraints in end-entity certificates. If it is included anyway, it MUST allow for an unlimited path length to allow the user to issue proxy certificates [14].

These two are the only values that are actually required.

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

The *nonRepudiation* (*contentCommitment*) value 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 is RECOMMENDED in order to enable use of the certificates with specific implementations of message-level security mechanisms where messages are to be encrypted[41].

The *keyCertSign* and *cRLSign* MUST NOT be set in an end-entity certificate, unless the certificate is explicitly intended for use in indirect CRL signing[42].

SHOULD Yellow

section 5 in footnote check it

3.3.3 *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* 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* as well as *clientAuth*[43]. [44].

[41] 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.

[42] See also section 2.4.2.

[43] 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.

[44] Refer to section 5 for all values that could be included in certificates.

OCSP responder certificates MUST have *oCSPResponder* asserted.

3.3.4 *nsCertType*

This extension is deprecated. It MUST NOT be used in new certificates; the appropriate equivalent values SHOULD be expressed in the *extendedKeyUsage* extension[45].

3.3.5 *nsPolicyURL*, *nsRevocationURL*

These attributes are deprecated and MUST NOT be used in end-entity certificates. If any of these extensions are included they MUST NOT be marked critical.

3.3.6 *nsComment*

This attribute is deprecated and SHOULD NOT be used in end-entity certificates[46]. If it is included, this extension MUST NOT be marked critical.

3.3.7 *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[47][48][49]. It MUST return the CRL in DER encoded form.

Some software[50] 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[51].

[45]The *extendedKeyUsage* and *nsCertType* extensions are interrelated and do 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*".

[46]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 RFC3280 RECOMMENDS that only an OID is used in the *certificatePolicies* extension. Also, compliant RFC 3280 implementations SHOULD actually display each and every user notice to the user.

[47]See also footnotes to section 2.4.5.

[48]Note that OpenSSL is not able to display the values of the reasons and the *CRLissuer* associated with a *DirectoryName* or URI.

[49]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.

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

[51]The http CRL URL will be downloaded extremely frequently. To allow for web caching of the CRL, it

3.3.8 *subjectKeyIdentifier*

The subjectKeyIdentifier extension MUST NOT be marked critical.

3.3.9 *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).

Possible attributes in AKI include the *directoryName* of the authority that issued the issuer certificate, which is safe to include as it should not change, as well as the serial number (which may or may 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.

3.3.10 *subjectAlternativeName*, *issuerAlternativeName*

Check footnote reference

The *subjectAlternativeName* 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* attribute. If an end-entity certificate needs to contain an rfc822 email address, this rfc822 address SHOULD be included as an *rfc822Name* attribute in this extension only.

For use with web server certificates, multiple FQDNs *dNSName* attributes can be added to allow name-based virtual hosting of secured web sites[52].

3.3.11 *authorityInformationAccess*

The *authorityInformationAccess* extension is the proper place to refer to any OCSP service that the issuer recommends validating software to used.

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 [4]. It is RECOMMENDED that the CRL be labelled with the correct MIME document type.

[52] See also footnote to section 3.4.3.

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 RFC4325, 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.

4 General Considerations

corrected spelling of representation

4.1 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 [11]), nor from sources such as the X.509 Style Guide [5]. The definition of the Name in X.501 [8] defines it as a SEQUENCE OF *RelativeDistinguishedName*, 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[53].

Unable to get a shaded box for verbatum for now

```
Name ::= SEQUENCE OF RelativeDistinguishedName

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

[53]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.

Un italicised SEQUENCE

italics in quotes in footnote qoute?

Since many authorization applications and namespace constraining policies are based on wildcard matching of only the trailing part of an OpenSSL one-line string representation rendering 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 issuing authority that issues end-entity certificates, or three or more trusted subordinate authorities[54].

4.2 Keys, key lengths and hashes

need to update the RSA statement

reference to url

Should this footnote be NOT RECOMMENDED to support non RSA algorithms

As explained in NIST special publication 800-57, 1024-bit RSA keys are 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 [1]. RSA claims that 1024-bit keys are likely to become crackable between 2006 and 2010 and that 2048-bit keys are sufficient until 2030 [12]. 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 [55]. 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[56].

footnote needs updating.

Similar considerations hold for the hash functions used, with the MD5 hash function known

[54]Discussions around the successor to RFC 3280 have included statements that the SEQUENCE ought to start with the Country or a domainComponent (still in draft). 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".

[55]See also `http://www.keylength.com`www.keylength.com for a comprehensive overview.

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

to have collisions, and SHA-1 having been shown to provide less than 80 bits of security. Thus, for the message digest that protects the certificate integrity, known-weak signatures or hash functions, such as MD5, MUST NOT be used in new certificates. The most secure hash function that is current supported by the entire target audience of the CA SHOULD be used, but at least SHA-1 or stronger MUST be used[57], with SHA-2 being recommended.

4.3 Maximum key lengths

RSA keys longer than 8192 bits have not been evaluated in production deployments. No EC keys have been evaluated in these environments either.

5 Directory Names and String Representations

correctly reference URL

Although comprehensive texts on the creation of certificate authorities and the configuration of particular CA software exist[58], 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:

[57] Note that modern hashes, such as SHA-256, are not supported by the majority of OpenSSL versions in use, so SHA-1 is the only available value as of time of writing.

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

For expressing these in OpenSSL, e.g., `http://www.math.ias.edu/doc/openssl-0.9.7a/openssl.txt`http://www.math.ias.edu/doc/openssl-0.9.7a/openssl.txt

RFC4514 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`

RFC4514 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:

RFC4514 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

RFC4514 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 of a grid 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

David G.: Please check this is correct.

Michael A. S Jones (Editor)
The University of Manchester
Mimas, Roscoe 5.9, The University of Manchester, Oxford Road
Manchester
United Kingdom
Email: mike.jones@manchester.ac.uk

8 Intellectual Property Statement

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] 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`.

[2] 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`.

[3] 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) Pro-

file. RFC 5280 (Proposed Standard), May 2008. URL http://www.ietf.org/rfc/rfc5280.txt. Updated by RFC 6818.

[4] 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.

[5] Peter Gutmann. X.509 style guide, October 2000. URL http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt.

[6] 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.

[7] R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280 (Proposed Standard), 2002. URL http://www.ietf.org/rfc/rfc3280.txt. Obsoleted by RFC 5280, updated by RFCs 4325, 4630.

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

[9] 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.

[10] 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.

[11] 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.

[12] Burt Kaliski. Twirl and rsa key sizes, May 2003. URL http://www.rsasecurity.com/rsalabs/node.asp?id=2004.

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

[14] 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`.