Randy Butler, NCSA
Tony J. Genovese, ESnet/LBNL

Global Grid Forum Certificate Policy Model

Status of This Memo

This memo provides information to the Grid community; it is a GGF community practice document. It does not define any standards or technical recommendations. Distribution is unlimited.

Copyright Notice

Abstract

This document describes a reference certificate policy (CP) for the operation of certificate authorities (CAs) within Grid environments. Specifically, the CP addresses the use of X.509 certificates for authentication but explicitly avoids documenting policies for digital signature and encryption. The goal of this CP is guide organizations in the deployment of public key infrastructure (PKI) to support technical interoperation with other Grid PKIs. This document serves as a model; it is written at times as if it were a policy, in order to give readers an example. In many cases suggestions and alternatives are given that readers will have to interpret on their own.

Sections of this document that have the phrase "No Stipulation" reflect the community's best practice. It does not imply that a CA cannot fill in these sections. It means only that at this time the community has not specified any requirements. Not all sections of the CP need to be filled in. It is the operator of the CA that must decide what is appropriate for his/her community.

Table of Contents

1 Introduction

This certificate policy (CP) was developed for the Global Grid Forum (GGF) community to reduce the cost and time needed to build a Grid public key infrastructure (PKI) and increase policy and technical interoperability in the Grid community. The document is a compilation of best practices and policies that will facilitate the deployment of a PKI for Grids that wish to facilitate interoperability with other Grids. The Global Grid Forum is not running a PKI for the GGF community; and although this document is written as if it were the certificate policy document for the Global Grid Forum, it is meant only as a *model* for those wishing to develop and document certificate policy for their Grid. This document does not preclude local Grids from extending the GGF CP to specify their own local Grid requirements, and indeed such extensions would be useful for a future refinement of this policy. It is expected, however, that this policy will be essential for the deployment of PKIs intending to support PKI interoperability and/or ease of integration of new sites into the particular Grid.

More information is available at http://www.gridforum.org/

This CP defines four certificate policies representing different assurance levels for public key digital certificates: rudimentary, basic, medium, and high. The word *assurance* used in this CP means how well a relying party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate, and how well the relying party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate.

The structure of this document is according to RFC 2527 [1]. Therefore some sections are maintained for compatibility, although they do not apply exactly to the services offered by all Grids. The Glossary section provides a glossary of terms used in this document. It is mainly based on [1].

Within this document the capitalized words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, and “OPTIONAL” are to be interpreted as in RFCs 2119 [2] (see Appendix).

In this document the expression “conforming CA” indicates a CA whose behavior conforms to the set of provisions specified in this document.

Finally, this CP has used the National Computational Science Alliance's [5] and the EuroPKI Certificate Policy [6] documents as initial source material.

1.1 Overview

This document describes a set of rules that indicates the applicability of a certificate issued by conforming CA to its community of users and/or class of application with common security requirements.

A certificate policy MAY be used by a certificate user to help in deciding whether a certificate, and the binding therein, is sufficiently trustworthy for a particular application. An X.509 Version 3 certificate issued by a conforming CA SHOULD contain a reference to this certificate policy.

More detailed information about the practices, which a conforming CA employs in its operations in issuing certificates, can be found in the Certificate Authorities Certification Practice Statements (CPS).

Every conforming CA MUST issue its own CP and CPS in order to provide information to potential clients of the CA about the underlying technical, procedural, and legal foundations that are not specified in this policy.

1.2 Identification

This is a GGF reference document and will not be assigned an object identifier (OID). It is recommended, however, that each CP have an OID assigned so that relying parties can verify the policies under which a certificate was generated.

1.3 Community and Applicability

A conforming CA can choose freely the community or communities it serves and applicability of their issued certificates, but it MUST clearly specify them in its own CP and CPS. In every case a conforming CA MUST NOT issue certificates to entities that don’t belong to its community or for applications that haven’t been carefully evaluated (for instance, high-value B2B transactions). Moreover, a conforming CA SHALL address all the limitations imposed by the following sections of this policy.

1.3.1 Certification Authority

An issuing conforming Certificate Authority (CA) must take particular care in deciding whether a particular organization or individual can manage a subject CA that performs all of the controls and checks detailed in this policy. A conforming CA MAY use as many registration authorities (RAs) as it wishes. A conforming CA MAY also have the role of RA if the CA itself can do the entity authentication. Subordinate CAs MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures.

1.3.2 Registration Authorities

Registration authorities (RAs) are useful for physical identification or authentication of entities. These authorities MUST NOT be permitted to issue certificates. The RA MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures as identified in the CA's certification practices statement (CPS).

1.3.3 End Entities

The end entities to be certified in accordance with this policy can be a person (individual or representing an organization) or a computational resource (e.g., a computer, a router, or an application) capable of performing cryptographic operations.

Each conforming CA MUST detail in its CP and CPS, who the end entities are, that it is willing to certify.

1.3.4 Applicability

One of the purposes of this policy is to promote wide use of public key certificates in many different applications. To promote interoperability, this policy strongly encourages CAs to support S/MIME for securing e-mail exchanges. It is also suggested that IPsec (to offer network layer security) and SSL/TLS (to offer transport layer security for protecting application protocols such as HTTP, Telnet, and FTP) SHOULD be supported. This policy in principle is not intended to put an a priori limitation on the use of the certificates except for the case in which certificates are used in a way that is prohibited by the law of the countries where the issuing CA is established. However, in order to evaluate whether certificates issued in accordance with

this policy are suitable for a certain application, Chapter 2 on "General Provisions" must be read carefully and fully understood.

The certificate levels of assurance contained in this CP are set forth in Table 1; also included in the table are examples of roles played by relevant personnel, as well as an indication of the number of distinct roles required.

Table 1: Certificate levels of assurance (In the last column, the numbers in brackets indicate the number of distinct roles required (for power separation reasons).

Assurance Level	**Risk**	**Roles**
Rudimentary	Low	[a] Account Administration, Key Generation, Maintain Audit Logs, Archive, Performing Backups, Issuing and Revoking Certificates
Basic	Moderate	[a] Account Administration, Key Generation, Maintain Audit Logs and Archive, Performing Backups; [b] Issuing and Revoking Certificates
Medium	Moderate	[a] Account Administration, Key Generation; [b] Issuing and Revoking Certificates; [c] Maintain Audit Logs and Archive, Performing Backups
High	Significant	[a] Account Administration and Key Generation; [b] Maintain Audit Logs and Archives; [c] Issuing and Revoking Certificates; [d] Performing Backups

EDITOR NOTE: in the above table the notation of a number within brackets might be interpreted as a reference. I changed the numbers to letters for this reason; alternatively you could use parentheses.

1.3.4.1 Rudimentary Assurance Level

The rudimentary level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. This level is not suitable for transactions requiring authentication and is generally insufficient for transactions requiring confidentiality, but it may be used for the

latter where certificates having higher levels of assurance are unavailable.

A single role is responsible for account administration, key generation, and maintenance of audit logs, archiving, backups, and issuing and revoking of certificates.

1.3.4.2 Basic Assurance Level

The basic level provides a level of assurance relevant to environments where there are risks and consequences of data compromise but they are not considered to be of major significance. It is assumed at this security level that users are not likely to be malicious.

This level requires, at a minimum, that CA personnel have two distinct roles. One role is responsible for account administration, key generation, audit, and archive configuration. The other role covers issuing and revoking of certificates.

This level of assurance increases the number of events that must be audited and requires increased cryptographic protection of audit logs, archives, and system backups.

1.3.4.3 Medium Assurance Level

The medium level is relevant to environments where risks and consequences of data compromise are moderate.

This level requires additional integrity controls to ensure data are not modified. It provides some protection against malicious authorized users by requiring additional role separation and more than one individual in a role to perform certain functions. This level requires, at a minimum, three distinct roles for CA personnel. One role is responsible for account administration, and key generation; a second role is responsible for issuing and revoking certificates; and a third role is responsible for maintaining the audit logs and archives and for performing backups.

The CA operating at this assurance level includes mechanisms to protect against someone with physical access to the components and includes additional requirements to ensure the CA is functioning securely. This level requires two-party control of private key export and additional

auditing of import and export of secret and private keys and requests for information.

1.3.4.4 High Assurance Level

The high level is appropriate for use where the threats to data are high or the consequences of the failure of security services are high.

This level of assurance is intended to protect against malicious authorized and unauthorized users by requiring, at a minimum, four distinct roles for CA personnel. One role is responsible for account administration and key generation; a second role is responsible for maintaining the audit logs and archives; a third role is responsible for issuing and revoking certificates; and a fourth role is responsible for performing backups.

This level requires significant assurance that the security features are functioning properly. It increases the integrity of audit logs and archives by requiring signed third-party time-stamping.

1.4 Contact Details

This section provides information administration of the CP and CPS.

1.4.1 Specification Administration Organization

This section MUST be used to document who administers the CP.

1.4.2 Contact Persons

This section MUST be used to document whom to contact concerning the CP.

1.4.3 Person Determining CPS Suitability for the Policy

Conforming CAs are responsible for establishing their own a policy management authority to oversee the CA. The PMA is responsible for setting policy, approving the CP and CPS, determining compliance with the CPS, and overseeing activities related to the development and enforcement of policy as specified in the CP.

2 General Provisions

This section describes obligations for relevant parties and discusses liability and financial and economic issues. Also included is a discussion about confidentiality, in which information is classified into two areas: confidential information and publicly available and distributable information. Auditing statements are also presented here.

2.1 Obligations

Obligations of the CA and the RA are described in this section.

2.1.1 CA Obligations

CAs are managed in general by a policy management authority. If the CA has a PMA, it is responsible for ensuring the CA obligations listed below.

Certificate authorities are responsible for all aspects of the issuance and management of a certificate referencing this policy, including the following:

- Development of a CP that is compliant with this reference model
- Development of a detailed statement of practices and procedures (the CPS) by which the CA implements the requirements of this policy
- Publication of CA contact information
- Certificate application and enrollment
- Verification of the identity of the applicant
- Certificate creation
- Posting of the certificate in a public repository
- Revocation of the certificate
- Certificate renewals
- Ensuring that all aspects of the CA services and CA operations and CA infrastructure related to certificates issued in accordance with this policy are performed in accordance with the requirements, representations, and warranties of this policy
- Ensuring that all certificates generated contain a reference to this policy in certificate extension field
- Definition and publication of a dispute resolution procedure
- Publication of CA audit results

By issuing a certificate that references this certificate policy, the CA certifies the following to the subscriber and to all qualified relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period:

- The CA has issued and will manage the certificate in accordance with this policy.
- The certificate has no misrepresentations of fact known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS.
- The certificate meets all material requirements of this certificate policy and CPS.

2.1.2 RA Obligations

An RA SHALL

- Validate the certificate request
- Authenticate the identity of the subject requesting certificate as documented in this certificate policy in Section 3
- Validate the connection between a public key and the requester identity, including a suitable proof of possession method
- Confirm such validation vs. the CA
- Adhere to the agreement made with the CA

2.1.3 Subscriber Obligations

In all cases, subscribers are required to

- Generate a key pair using a trustworthy method
- Review and verify accuracy of their representations included in the published certificate
- Use the certificate exclusively for authorized and legal purposes, consistent with this policy
- Instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscribers private key
- Take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key associated with the

- certificate, such as (1) selecting a pass phrase that is a minimum 16 characters, (2) using upper and lower characters or special characters in the pass phrase, and (3) protecting the pass phrase (private key) from others.

2.1.4 Relying Party Obligations

Qualified relying parties are expected to rely on certificates that reference this policy as appropriate authentication of the subscriber under the following conditions:

- The relying party is familiar with the CPS of the CA that generated the certificate and with the certificate policy before drawing any conclusion on trust of a certificate issued from a conforming CA.
- The reliance is reasonable and in good faith in light of all the circumstances known to the relying party at the time of reliance.
- The purpose for which the certificate was used was appropriate in accordance with this policy.
- The relying party checked the status of the certificate prior to reliance, or a check of the certificate's status would have indicated that the certificate was valid.
- The reliance is for lawful purposes.

2.1.5 Repository Obligations

Each conforming CA should use a publicly accessible repository to store certificates and certificate revocation lists.

The repository should be available 24/7.

2.2 Liability

This section discusses the liability of the CA and the RA.

2.2.1 CA Liability

The Global Grid Forum assumes no liability for any direct or indirect damages suffered by relying parties caused by the failure of the CA to comply with either its policy or CPS or resulting from the reliance of a relying party on a certificate issued by the CA.

A conforming CA MAY accept liability. Since this policy is established primarily to promote the adoption of certificates as a means to increase computer and network security in a broad variety of applications, there is no a priori limitation to applicability of certificates issued in accordance with this policy (see Section 1.3.4). Therefore, if no limitation is put on certificate applicability, this policy suggests that CA liability is restricted to the guarantee of making the necessary controls to verify the identity of every requester as described in the CP and CPS and to the adoption of the minimal security measures needed to protect a CA's private key. In every case the complete list of accepted liabilities MUST be specified in the CPS.

2.2.2 RA Liability

RA liability is covered in Section 2.2.1.

2.3 Financial Responsibility

With regard to what is stated in Sections 1.3.4, 2.2.1, and 2.5, no financial responsibility is accepted for certificates issued in accordance with the certificate policy.

2.3.1 Indemnification by Relying Parties

Indemnification by relying parties must be defined in the CP and CPS.

2.3.2 Fiduciary Relationships

Fiduciary relationships must be defined in the CP and CPS.

2.3.3 Administrative Processes

Administrative processes must be defined in the CP and CPS.

2.4 Interpretation and Enforcement

This section covers the responsibilities of the CA and the actions to be taken if the CA ceases operation.

2.4.1 Governing Law

Interpretation of this policy is according to the law of the country in which the conforming CA is established. This MUST be detailed in the CP and CPS.

2.4.2 Severability, Survival, Merger, Notice

If the CA ceases operation, the CA must promptly notify all subscribers, sponsoring organizations, RAs, RSPs, and qualified relying parties of the termination.

In addition, the CA must promptly notify all CAs with which cross-certification agreements current at the time of cessation of the termination.

All certificates issued by the CA that reference this policy will be revoked no later than the time of termination.

2.5 Dispute Resolution Procedures

The CA must define a dispute resolution procedure within the CP and CPS and publish it in a publicly accessible place.

2.6 Fees

Discussed in this section are those cases in which the CA is or is not allowed to charge fees.

2.6.1 Certificate Issuance or Renewal Fees

This policy suggests that no fees are charged for issuing certificates. The CA MAY charge fees, but this charge MUST explicitly be stated in the CP and CPS.

2.6.2 Certificate Access Fees

This policy suggests that no fees are charged for allowing certificate access. The CA MAY charge fees, but this charge MUST explicitly be stated in the CP and CPS.

2.6.3 Revocation or Status Information Access Fees

Fees MUST NOT be charged for allowing certificates revocation or status information access.

2.6.4 Fees for Other Services

Fees MUST NOT be charged for allowing policy and CPS information access.

2.6.5 Refund Policy

The refund policy MUST be defined in the CP and CPS.

2.7 Publication and Repository

CA information will involve considerable documentation. This section discusses how these documents are to be handled.

2.7.1 Publication of CA Information

Each authorized CA SHALL operate a secure on-line repository that is available to qualified relying parties and that contains the following:

- Audit results
- Certificates issued that reference this policy
- Signed certificate revocation list or on-line certificate status database for certificates issued reference this policy
- All issued certificates except those certificates of subscribers that explicitly requested that their certificate not be made publicly available
- The CA's certificate for its signing key
- Past and current versions of the CA's CPS
- A copy of this policy
- Other relevant information relating to certificates that reference this policy

2.7.2 Frequency of Publication

Certificates MUST be published as soon as they are issued. The frequency of CRL publication is specified in Section 4.4.9. Also, policy and CPS SHALL be published as soon as they are updated.

2.7.3 Access Control

There SHOULD be no access control to policy, CPS, and CRL. There MAY be access control to certificates (for instance, to prevent bulk acquisition of data such as e-mail addresses or when CA decides to charge fees for certification services).

2.7.4 Repositories

There MUST exist at least a repository for publishing the information mentioned above.

2.8 Compliance Audit

To develop trust in the CA, relying organizations usually require an audit of the facilities and operations of the CA to ensure that it is complying with the CP. This audit could entail the use of third-party auditors. In many GGF PKIs these audits are done by peer PKIs. Peer review is the process that the European Data Grid and the DOE Grids d to evaluate their member organizations; third-party audits were considered too expensive for the level of trust that was required.

2.8.1 Frequency of Entity Compliance Audit

Audits are done before initial approval as an Authorized CA, and thereafter at least once every year.

2.8.2 Identity and Qualifications of Auditor

The auditing team comprises members representing applications, infrastructure, and policy/management activities not affiliated with the CA or the organization that manages the CA.

2.8.3 Auditor's Relationship to Audited Party

The auditor's relationship to audited party MUST be defined in the CP and CPS. The auditors MUST NOT be affiliated with the CA or the organization that manages the CA.

2.8.4 Topics Covered by Audit

The audit evaluates the quality of the services provided by the CA. The audit determines whether the CA complies with all of the requirements

of this policy and its CPS and whether the CPS CP and CPS are consistent with the requirements of this policy.

2.8.5 Deficiency

If a CA fails an audit, a relying party may refuse to accept certificate from the CA. If the CA is a subordinate of another, it may lose its right to issue certificates under the superior CA.

2.8.6 Communication of Results

Procedures for communicating the results of an audit MUST be defined in the CP and CPS. Results (pass/fail) of CA audits are to be made public and posted on the Global Grid Forum Web site.

2.9 Confidentiality

The CA collects personal information about the subscribers (e.g., full name, organization, and e-mail address). This information MUST be processed in a way that ensures privacy protection according to the laws of the country where the CA is established.

2.9.1 Confidential Information

All subscribers' information that is not present in the certificate and certificate revocation list (CRL) issued by a conforming CA is considered confidential and SHALL NOT be released outside without explicit and well-documented subscriber's authorization.

Under no circumstances SHALL the CA (or any other entity involved in the certificate administration process) have access to the private keys of any subscriber to whom it issues a certificate that references this policy.

2.9.2 Information Not Considered Confidential

Information included in public certificates and CRLs issued by a conforming CA is not considered confidential.

2.9.3 Certificate Revocation or Suspension Information

When a certificate is revoked or suspended, a reason code MAY be included in the CRL entry for the action. This reason code is not

considered confidential and may be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed.

2.9.4 Release to Law Enforcement Officials

A conforming CA will not disclose certificate or certificate-related information to any third party, except when required by law enforcement officials having a regular warrant.

2.9.5 Release as Part of Civil Discovery

Disclosure of certificate or certificate-related information as part of civil discovery MUST be defined in the CP and CPS.

2.9.6 Disclosure upon Owner's Request

A conforming CA will not disclose certificate or certificate-related information to any third party except when required by the owner, with a signed request.

2.9.7 Other Information Release Circumstances

Other cases in which information may or may not be released MUST be defined in the CP and CPS.

2.10 Intellectual Property Rights

A conforming CA MUST NOT claim any intellectual property rights (IPRs) on issued certificates.

3 Identification and Authentication

This section describes the procedures used to identify and authenticate a certificate requester to a CA or RA before certificate issuance. It also describes how parties requesting rekey or revocation are authenticated. In addition, this section addresses naming practices, including name ownership recognition and name dispute resolution.

3.1 Initial Registration

Policies regarding selection and specification of names are presented in this section.

3.1.1 Types of Names

The naming attributes of the subscriber to be requested to identify and authenticate the requester depend on the type of certificate that the subscriber requires. In the choice of the types and format of names used in the certificate fields, Global Grid Forum policy conforms to RFC 2459 [3].

A conforming CA MUST detail in the CP and CPS the types and format of names used.

3.1.2 Meaningful Names

The subject and issuer names contained in a certificate MUST be meaningful in the sense that the issuing CA has proper evidence of the association between these names and the entities to which they belong.

If an e-mail address is included in the certificate, it need not follow a semantic rule that could be used to identify person and/or organization.

3.1.3 Interpretation of Name Forms

A conforming CA MUST detail in the CP and CPS the rules for interpreting various name forms used in the certificates.

3.1.4 Uniqueness of Names

The DN (Distinguished Name) MUST be unique for each subject entity certified by the one CA as defined by the issuer name field.

3.1.5 Name Claim Dispute

Disputes are managed according to the law of the country where the CA is established.

3.1.6 Trademarks

Policies for recognition and authentication of trademarks MUST be defined in the CP and CPS.

3.1.7 Proof of Possession of Private Key

A method must be adopted for proving possession of the private key corresponding to the public key being certified.

The method adopted MUST be detailed in the CP and CPS. A conforming CA MUST NOT issue a certificate for which the proof of possession fails. This policy discourages generation of a private key by the issuing CA as a proof of possession.

3.1.8 Authentication of Organization Identity

Every time a subscriber requires the inclusion of the name of a certain organization in a certificate, the issuing CA MUST have evidence (documentation) that the organization has complete knowledge about this fact. In all cases suitable legal documents that prove the data to be certified MUST be presented to the CA. The CA or RA MAY perform the authentication. The details MUST be specified in the CP and CPS.

3.1.9 Authentication of Individual Identity

In many cases public key certificates constitute a means to guarantee strong cryptographic authentication of communicating entities. Bearing in mind this premise, this policy REQUIRES the authentication of individual identity. The RECOMMENDED method of authentication requires that individual to present personally to the authenticating CA or RA suitable identification documents. Other methods, such as videoconference, MAY be adopted. If the subject to be certified is a software component, the person who submits the request MUST prove that he or she has the necessary authorization. The procedure MUST be detailed in the CP and CPS.

For subscribers, the CA SHALL ensure that the applicant's identity information is verified in accordance with the applicable CP and CPS. CAs or RAs SHALL ensure that the applicant's identity information and public key are bound adequately. Additionally, CAs or RAs SHALL record the process that was followed for issuance of each certificate. Process information SHALL depend on the certificate level of assurance and SHALL be addressed in the CP and CPS. It is RECOMMENDED that the process documentation include the following as a minimum for proving identity, except for the rudimentary level of assurance:

- The identity of the person performing the identification

- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable certificate policy
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant
- The date and time of the verification
- A declaration of identity. The declaration SHALL be signed with a handwritten signature by the certificate applicant; if in-person identity-proofing is done, this SHALL be performed in the presence of the person performing the identity authentication. Where the applicant is not a human being but is instead a network device or some other entity, the requirements pertaining to identity proofing SHALL be done through the human owner or designated representative.

Some of the following text is drawn from CPs operating within the United States and therefore may not be applicable to other countries. Every CP needs to comply with the local privacy and identity law of the country in which the CA is operated. The following are examples of authentication identification requirements for the four levels of assurance.

Rudimentary: The applicant may apply in person, or through a network (such as the Internet), or by correspondence.

No proof of the applicant's identity is required.

The private key corresponding to the public key offered for the certificate may exist in any software or hardware form. The certificate SHALL contain either a non-null subject name or, if a null subject name, an alternative subject name that is populated and marked as non-critical.

This level is intended only for ensuring data integrity checking. In particular, this level is considered valid for use in testing but not for production Grids.

Basic: The applicant MAY apply in person or through a network (such as the Internet). If a network is used, the connections between the applicant and the registration authority or its designated representative (for registration) and certification authority (for transport of the public key for certificate issuance) SHALL be secured by using a protocol defined in the certification practice statement

that provides for strong encryption for the transferring of information.

The applicant SHALL provide appropriate proof of identity, and the RA SHALL vet the information to confirm identity. This MAY be done through use of a database or by attestation from a trusted individual in the same organization.

The private key corresponding to the public key offered for the certificate MAY exist in software or a hardware token, and its possession by the applicant SHALL be proven in accordance with PKIX Certificate Management Protocol or an equivalent protocol defined in the certification practice statement. The certificate SHALL contain a non-null subject name and MAY contain an alternative subject name marked as non-critical.

Medium: The applicant SHALL appear in person before the registration authority, a trusted agent approved by the RA as being authorized to confirm identities (such as a notary public), that uses a stamp, seal, or other mechanism to confirm that it has authenticated the identity of the applicant.

The applicant SHALL present at least one government-issued official picture identification credential, or two non-government-issued official identification credentials, at least one of which must be a photo I.D., such as a driver's license. As an alternative to presentation of identification credentials, other mechanisms of equivalent or greater assurance may be used, such as comparison of biometric data to identities pre-verified to the standards of this CP, obtained via authenticated interaction with secured databases.

The registration authority or its designated representative SHALL personally verify the applicant's identity, or the applicant SHALL provide credential information that required an in-person appearance before an entity accepted by the registration authority. For example, if the applicant has a credential that was digitally signed by an entity accepted by the registration authority and that required the applicant to make an in-person appearance before that entity, that credential may be accepted on-line along with other information without necessitating an in-person appearance before the registration authority. The certificate SHALL contain a distinguished name and may contain an alternative subject name if marked as noncritical.

When a private key is delivered to a subscriber via a hardware token, the subscriber SHALL personally appear before the RA or trusted agent to obtain the token or token activation data.

The private key corresponding to the public key offered for the certificate MAY exist in software or a hardware token. Its possession by the applicant SHALL be proven in accordance with PKIX Certificate Management Protocol or an equivalent protocol defined in the Certification Practice Statement (CPS). The certificate SHALL contain an X.500 distinguished name and MAY contain an alternative subject name if marked as noncritical.

High: The applicant SHALL appear in person before the registration authority or a trusted gent approved by the RA.

The applicant SHALL present at least one government-issued official picture identification credential or two nongovernment-issued official identification credentials, at least one of which must be a photo I.D., such as a driver's license. As an alternative to presentation of identification credentials, other mechanisms of equivalent or greater assurance may be used, such as comparison of biometric data to identities preverified to the standards of this CP, obtained via authenticated interaction with secured databases.

When a private key is delivered to a subscriber via a hardware token, the subscriber SHALL personally appear before the RA or trusted agent to obtain the token or token activation data.

The private key corresponding to the public key offered for the certificate SHALL exist in a hardware token. Its possession by the applicant SHALL be proven in accordance with PKIX Certificate Management Protocol or an equivalent protocol defined in the certification practice statement. The certificate SHALL contain an X.500 distinguished name and MAY contain an optional alternative subject name if marked as noncritical.

For All Levels: Applicants who are unable to perform face-to-face registration alone (e.g., a network device) SHALL be represented by a trusted person already issued a digital certificate by the agency. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself and the applicant who the trusted person is representing.

Table 2 summarizes the identification requirements for each level of assurance.

Table 2: Identification requirements for levels of assurance

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his e-mail address
Basic	Identity may be established by in-person appearance before a registration authority or designated representative; or by comparison of user-supplied information (on-line or in-person) to a database.
Medium	Identity established by in-person appearance before the registration authority, trusted agent, or designated representative. Credentials required are either one government-issued picture I.D. or two nongovernment I.D.s, one of which SHALL be a photo I.D. (e.g., driver's license)
High	Identity established by in-person appearance before the registration authority or trusted agent. Credentials required are either one government-issued picture I.D. or two nongovernment-issued I.D.s, one of which SHALL be a photo I.D. (e.g., driver's license)

3.2 Routine Rekey

This policy does not mandate any compulsory rekey. After certificate expiration, the CA MAY issue a new certificate for the same key or for a new key. The rekey authentication MAY be accomplished with the same procedure indicate in Section 3.1 for initial registration or by using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

A CA MAY issue more than one certificate for the same subscriber with the same key.

Table 3: Rekey Requirements

Assurance Level	Routine Rekey Requirements for End-Entity Subscriber Signature and Encryption Certificates
Rudimentary	Rekey SHALL be accomplished during the lesser of (a) 100 days prior to key expiry or (b) the final 10% of the validity period for the current signature key Identity may be established through use of current signature key
Basic	Rekey SHALL be accomplished during the lesser of (a) 100 days prior to key expiry or (b) the final 10% of the validity period for the current signature key Identity may be established through use of current signature key, except that identity SHALL be reestablished through initial registration process at least once every 15 years from the time of initial registration
Medium	Rekey SHALL be accomplished during the lesser of (a) 100 days prior to key expiry or (b) the final 10% of the validity period for the current signature key Identity may be established through use of current signature key, except that identity SHALL be established through initial registration process at least once every 10 years from the time of initial registration
High	Rekey SHALL be accomplished during the lesser of (a) 100 days prior to key expiry or (b) the final 10% of the validity period for the current signature key Identity must be established in person in accordance with initial registration process.

3.3 Rekey after Revocation

A public key whose certificate has been revoked for private key compromise MUST NOT be recertified. The public key MAY be recertified if the revocation is due to certificate suspension. In the latter case the rekey authentication MAY be accomplished with the same procedure indicated in Section 3.1 for initial registration or by using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

3.4 Revocation Request

A proper authentication method is required in order to accept revocation request. A conforming CA MUST accept as a revocation request a message digitally signed with a valid certificate issued in

accordance with this policy. The same procedures adopted for the authentication during initial registration are also considered suitable. Alternative procedures MAY be supported, such as secure communication of a revocation Personal Identification Number (PIN). The exact procedures supported MUST be detailed in the CP and CPS. See Section 4.4.2.

4 Operational Requirements

This section specifies requirements imposed on entities involved in the certification and certificate revocation process.

4.1 Certificate Application

This policy permits two procedures for certificate application:

- Certification of entities done entirely by the CA. The details about this procedure MUST be specified in the CP and CPS.
- An entity generates its own key pair and submits public key and other required data to the CA. After that, the request MUST carefully follow the procedures detailed in this policy and in the CP and CPS for identification and authentication.

4.2 Certificate Issuance

Conforming CA and RA MUST carefully check the compliance and validity of documents presented by the subscribers. After authentication as specified in Section 3.1, CA SHOULD issue the certificate. In the case of issuance CA MUST notify the requester. If for any reason CA decides not to issue the certificate (even if the checks and the authentication were correct) it SHOULD notify the requester of the reason for this decision.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

A conforming CA is responsible for issuing CRLs and for publishing signed versions. Although RFC 2459 [3] does not require CAs to issue CRLs, a conforming CA MUST issue timely CRLs.

The CA MUST update its CRL with revoked subject CA certificates.

4.4.1 Circumstances for Revocation

A certificate MUST be revoked when information in the certificate is known to be or suspected of being compromised. Such situations include the following:

- The subscriber's data changed.
- The subscriber's private key is compromised or is suspected to have been compromised.
- The subscriber's information in the certificate is suspected to be inaccurate.
- The subscriber is known to have violated his obligations.

4.4.2 Request for Revocation

A conforming CA MUST accept a revocation request made by the holder of the certificate to be revoked. The revocation request MAY come from the CA that issued the certificate or from an associated RA.

Other entities MAY require revocation, presenting evident proof of knowledge of the private key compromise or the change of subscriber's data.

4.4.3 Procedure for Revocation Request

The entity requesting the revocation MUST be properly authenticated. The authentication method SHOULD be as strong as the one used in the issuing procedure. A conforming CA MUST accept as a revocation request a message digitally signed with a "not expired and not previously revoked" certificate issued in accordance with this policy. An alternative procedure MAY require the entity to visit the RA or CA and to present a viable identity document.

If the entity is a CA, the CA MUST, in addition,

- Inform subscribers and cross-certifying CAs
- Terminate the certificate and CRLs distribution service for certificates or CRLs issued using the compromised private key.

4.4.4 Revocation Request Grace Period

The conforming CA decides the amount of time necessary to accept the request.

4.4.5 Circumstances for Suspension

A CA MAY temporarily suspend a subscriber's certificate if the subscriber requests that service. Unlike revocation, suspension of a user allows for re-enabling at a later time. In every case, the conforming CA is not required to offer the suspension service. Information on public keys of disabled users MAY be available from the CA repository.

4.4.6 Request for Suspension

If a CA offers the suspension service, the CA MUST accept a suspension request made by the holder of the certificate to be suspended.

4.4.7 Procedure for Suspension Request

The entity requesting the suspension MUST be properly authenticated. A conforming CA MUST accept as a suspension request a message digitally signed with a "not expired and not previously revoked" certificate issued in accordance with this policy. An alternative procedure MAY require the entity to visit the RA or CA and to present a viable identity document.

4.4.8 Limits on Suspension Period

No stipulation.

4.4.9 CRL Issuance Frequency

CRLs MUST be updated within one hour of receiving and validating a certificate revocation request. CRLs MUST be reissued at least every 40 days by conforming CA.

4.4.10 CRL Checking Requirements

A relying party MUST verify a certificate against the most recent CRL issued from conforming CA in order to validate the use of the certificate.

4.4.11 On-Line Revocation and Status Checking

A conforming CA MAY support on-line revocation/status checking. Although this policy requires conforming CA to issue CRL, it is not mandatory to implement on-line revocation and status checking procedures. However, this policy suggests taking into consideration OCSP [4] as such a mechanism.

4.4.12 On-Line Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisements

No stipulation.

4.4.14 Checking Requirements for Other forms of revocation advertisements

No stipulation.

4.5 Security Audit Procedures

This policy recognizes the importance of security audit procedures suggesting that conforming CA specifies all this kind of provisions in the CP and CPS.

4.5.1 Types of Event Recorded

No stipulation

4.5.2 Frequency of Processing Log

No stipulation

4.5.3 Retention Period for Audit Log

No stipulation

4.5.4 Protection of Audit Log

No stipulation

4.5.5 Audit Log Backup Procedures

No stipulation

4.5.6 Audit Collection System (Internal vs External)

No stipulation

4.5.7 Notification to Event-Causing Subject

No stipulation

4.5.8 Vulnerability Assessments

No stipulation

4.6 Records Archival

This section specifies the types of event recorded for archival purposes from the CA and RA and how this collected data are maintained. For further details not explicitly stipulated here, the reference is the CPS.

4.6.1 Types of Event Recorded

A conforming CA SHOULD archive the following:

- Certification requests corresponding to actually
- Issued certificates
- Issued CRLs
- All signed agreements with other parties (e.g., RA)
- Document collected from the subscriber during the enrollment procedure
- All relevant messages exchanged with the RA

The RAs SHOULD archive the following:

- All validation information collected from the subscriber

- All relevant messages exchanged with the CA

4.6.2 Retention Period for Archive

The minimum retention period is two years.

4.6.3 Protection of Archive

No stipulation

4.6.4 Archive Backup Procedures

No stipulation

4.6.5 Requirements for Time-Stamping of Records

No stipulation

4.6.6 Archive Collection System (Internal or External)

No stipulation

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation

4.7 Key Changeover

No stipulation

4.8 Compromise and Disaster Recovery

If a CA's private key is compromised or suspected to have been compromised, the CA MUST at least do the following:

- Inform subscribers, cross-certifying CAs and relying parties
- Terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key
- Request the revocation of the CA's certificate.

If a RA's private key is compromised or suspected to have been compromised, the RA SHALL at least inform the CA and request the revocation of the RA's certificate.

If an entity's private key is compromised or suspected to have been compromised, the entity SHALL at least inform the relying parties and request the revocation of the entity's certificate.

4.8.1 Computing Resources, Software, and/or Data Are Corrupted

No stipulation

4.8.2 Entity Public Key Is Revoked

No stipulation

4.8.3 Entity key Is Compromised

No stipulation

4.8.4 Secure Facility after Disaster

No stipulation

4.9 CA Termination

Termination of a CA is the situation in which all service associated with a logical CA is terminated permanently.

Before the CA terminates its services, the following procedures MUST be completed as a minimum:

- Inform all subscribers, cross-certifying CA's, higher-level CAs, and relying parties with which the CA has agreements or other form of established relations.
- Make publicly available information of its termination.
- Stop distributing certificates and CRLs.
- Destroy private keys and all copies.

A subordinate CA MUST terminate. It could reestablish itself as a self-standing CA. The subordinate could reuse its key pair as a self-signed certificate.

5 Physical, Procedural, and Personnel Security Controls

This section discusses security requirements pertaining to resource use, roles, and personnel.

5.1 Physical Controls

Security requirements imposed on the conforming CA are indicated in the CPS. In every case this policy states that CA MUST be run on a dedicated workstation. The workstation MUST be physically secured.

5.1.1 Site Locations and Construction

No stipulation

5.1.2 Physical Access

The physical access to the site in which the CA operates MUST be restricted only to explicitly authorized people.

5.1.3 Power and Air Conditioning

No stipulation

5.1.4 Water Exposure

No stipulation

5.1.5 Fire Prevention and Protection

No stipulation

5.1.6 Media Storage

No stipulation

5.1.7 Waste Disposal

No stipulation

5.1.8 Off-Site Backup

Off-site backup facilities, if used, MUST be secured to allow access only to authorized personnel.

5.2 Procedural Controls

All the issues related to procedural control, such as the definition of trusted roles, MUST be specified in the CP and CPS.

5.2.1 Trusted Roles

No stipulation

5.2.2 Number of Persons Required per Task

No stipulation

5.2.3 Identification and Authentication for Each Role

No stipulation

5.3 Personnel Controls

This section is devoted to requirements and procedures for personnel.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

The personnel operating the CA MUST be technically and professionally competent. Every conforming CA MUST specify in the CP and CPS further details concerning this particular topic and the related issues.

5.3.2 Background Check Procedures

No stipulation

5.3.3 Training Requirements

No stipulation

5.3.4 Retraining Frequency and Requirements

No stipulation

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

No stipulation

5.3.7 Contracting Personnel Requirements

No stipulation

5.3.8 Documentation Supplied to Personnel

No stipulation

6 Technical Security Controls

This section defines the provisions for key management and the corresponding technical security controls.

6.1 Key Pair Generation

A conforming CA's cryptographic keys are generated by the package chosen for certificate handling. End entities' cryptographic keys are locally generated by their application during the requesting process or by the CA during the enrollment procedure. This policy suggests the adoption of the former procedure for signing key pair to be used for non-repudiation purposes. The latter procedure MAY be adopted for encryption key pair or bulk authentication key pair.

6.2 Private Key Delivery to Entity

The entity MAY generate his own key pair. If the CA generates the key pair, that key pair MUST be given to the end entity in a secure way. Further details MUST be specified in the CP and CPS.

6.3 Public Key Delivery to Certificate Issuer

For individual certification, the entity MUST submit to the CA or RA a certification request containing the public key, locally generated. Every conforming CA MUST specify in its CPS the exact procedures for delivering public key. For CA certification, the subject CA generates the key pair.

6.4 CA Public Key Delivery to Users

A conforming CA MUST provide mechanisms to deliver CA public key to the users in a trustworthy manner. Further details MUST be specified in the CP and CPS. In every case, the CA's public keys MUST be publicly available in a repository accessible via a standard protocol such as HTTP or LDAP.

6.5 Key Size

The minimum length of the private key of an end entity to be certified MUST be decided by the CA issuer. It is RECOMMENDED that the PMA sets minimum key size based on the vulnerability of the key to compromise by brute strength. This minimum key length value should be reviewed on a regular basis and modified as required.

6.6 Generation of Public Key Parameters

No stipulation

6.7 Parameter Quality Checking

No stipulation

6.8 Generation of Hardware/Software Key

The keys can be generated in software or in hardware (e.g., on a cryptodevice) depending on the various tools available to the entities.

6.9 Key Usage

The key usage is specified in the X.509 v3 KeyUsage field. This field indicates the purpose for which the certified public key is used. Certificates issued in accordance with this policy MUST have the KeyUsage extension flagged as critical. In other words, the certificate

MUST be used only for a purpose for which the corresponding key usage bit is set to one.

A CA, through the KeyUsage extension in the certificate, MAY restrict the purposes for which a key can be used.

7 CA Certificates

In a CA's certificate, the KeyUsage extension MUST be specified in the CP or CPS.

7.1 Private Key Protection

This section discusses policies for protecting, archiving, and retrieving or destroying private keys, both of individuals and of groups.

7.1.1 Standards for Cryptographic Module

This policy does not mandate the adoption of a cryptographic module compliant with predetermined standards. Every conforming CA MAY give in the CP and CPS more details about the adoption of standard compliant module.

7.1.2 Private Key Multiperson Control

The private key of individual MUST NOT be under (n out of m) multiperson control. Only private keys belonging to a CA, a hardware component, or a software component MAY be under such a control: in this case the type of control MUST be specified in the CP and CPS.

7.1.3 Private Key Escrow

This policy discourages the implementation of private key escrow policy both for end entities and for CAs.

7.1.4 Private Key Backup

All the parties SHOULD maintain a backup copy of the private key in order to reconstitute it in case of destruction of the key. This backup MUST be carefully protected, especially in the case of backup of private key CA.

7.1.5 Private Key Archive

This policy suggests the implementation of a procedure for private key archive only for a private key used for encryption/decryption. Indeed, it MAY be necessary to maintain a copy of a private key in order to correctly decrypt messages even if the corresponding public key certificate is expired.

7.1.6 Private Key Entry into a Cryptographic Module

The private key of all entities SHOULD be stored in an encrypted form. This provision is particularly important if the entity is a CA.

7.1.7 Activating a Private Key

Specific details about how to activate a private key SHOULD be found in the CP and CPS. For the activation of a private key some specific activation data MUST be entered in the cryptographic module. At least the activation data MUST consist in a PIN or pass phrase, but for the most valuable private key (e.g., the ones belonging to CA) the use of hardware tokens or biometrics data is suggested.

7.1.8 Deactivating a Private Key

No stipulation

7.1.9 Destroying a Private Key

No stipulation

7.2 Other Aspects of Key Pair Management

This section focuses on archiving of public keys.

7.2.1 Public Key Archival

Conforming CA MUST archive all issued certificates. Mechanisms to provide integrity controls other than digital signatures MAY be implemented.

7.2.2 Usage Periods for Public and Private Keys

No stipulation

7.3 Activation Data

This section discusses generation, installation, and protection of activation data.

7.3.1 Activation Data Generation and Installation

Pass phrases or PINs MUST be selected according to "best practice." Hence, a suitable minimal length for the pass phrases must be suggested and mechanisms established to check that pass phrases show enough entropy.

7.3.2 Activation Data Protection

Pass phrases protecting private keys MUST be accessible only to the legitimate users (e.g., certificate holder for personal certificates, CA operators for CA signing keys). An exception for this indication is the implementation of a secure archival/backup mechanism for activation data. Such a mechanism MUST be clearly defined in the CP and CPS.

7.3.3 Other Aspects of Activation Data

No stipulation

7.4 Computer Security Controls

Currently, no policies have been established for computer security controls.

7.4.1 Computer Security Technical Requirements

No stipulation

7.4.2 Computer Security Rating

No stipulation

7.5 Life-Cycle Technical Controls

Currently, no policies have been established for life-cycle technical controls.

7.5.1 System Development Controls

No stipulation

7.5.2 Security Management Controls

No stipulation

7.5.3 Life-Cycle Security Rating

No stipulation

7.6 Network Security Controls

The machine on which the cryptographic module used for CA operations SHOULD be kept off-line to prevent network attacks. In every case network access to the CA workstation MUST be limited in order to protect the CA's private key from disclosure.

7.7 Cryptographic Module Engineering Controls

No stipulation

8 Certificate and CRL Profiles

This section briefly discusses policies for certificate and CRL profiles.

8.1 Certificate Profile

This topic will be covered in a separate GGF best practices document. Refer to that document for guidance.

8.2 CRL Profile

Policies for CRL profiles are outlined below.

8.2.1 Version Number(s)

Those deploying Grids have determined that the version field in the certificate should stat 1, indicating X.509.v2 CRL.

8.2.2 CRL and CRL Entry Extensions

No stipulation.

9 Administration of Specifications

Specifications require review, notification, and approval. Each of these topics is discussed in this section.

9.1 Specification Changes

Editorial changes can be made to the policy and CPS. In case of substantial changes in the policy, all CAs and users MUST be notified in advance. Moreover, CAs MUST update the policy in accordance with the policy changes. Policy changes that imply minor technical adjustments MUST be declared in advance.

9.2 Publication and Notification Policies

This policy will be published and made available on-line as a GGF document and maintained as part of the GGF document store.

9.3 CPS Approval Procedures

A conforming CA MUST be evaluated for compliance with the policy. In order to obtain CPS approval, a conforming CA MAY submit its CPS to the contact people specified in Section 1.4.3. After that, the conforming CA MUST wait for the answer. The time limit for completing the evaluation is 60 days. It might be acceptable to have CA self-certification for compliance, but in this case if noncompliance is reported to the Global Grid Forum, then the CA certificate will be revoked.

10 Security Considerations

Each PKI that runs a CA must consider its security at all levels: network, system and software. Many appropriate guidelines are available

on each of these topics. The trust between PKIs will be influenced greatly by the security considerations of the implementing site.

11 Author Information

Randy Butler
NCSA
RButler@ncsa.uiuc.edu

Tony J. Genovese
ESnet/LBNL
Tony@ES.net

12 Glossary

Certification authority (CA) – An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. The CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA certificate – A certificate for one CA's public key issued by another CA.

Certificate policy (CP) – A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path – An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification practice statement (CPS) – A statement of the practices that a certification authority employs in issuing certificates.

Certificate revocation list (CRL) – A time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.

Issuing certification authority (issuing CA) – The CA that issues the certificate (see also Subject certification authority).

Public key certificate (PKC) – A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA that issued it.

Public Key Infrastructure (PKI) - The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public key cryptography.

Registration authority (RA) - An entity that is responsible for identification and authentication of certificate subjects but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). The term Local Registration Authority (LRA) is used elsewhere for the same concept.

Relying party - A recipient of a certificate who acts in reliance on that certificate or on digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate.

IPR – Intellectual property rights

13 Intellectual Property Statement

The GGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the GGF Secretariat.

The GGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to practice this recommendation. Please address the information to the GGF Executive Director.

14 Full Copyright Notice

15 Appendix

Key Words in RFCs to Indicate Requirement Levels

RFC 2119 [2], "Key Words for Use in RFCs to Indicate Requirement Levels" specifies how the main key words used in RFCs should be interpreted. Authors who follow these guidelines should incorporate the following statement near the beginning of their document:

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

1. **MUST –** This word, or the terms "REQUIRED" or "SHALL," mean that the definition is an absolute requirement of the specification.

2. **MUST NOT –** This phrase, or the phrase "SHALL NOT," means that the definition is an absolute prohibition of the specification.

3. **SHOULD –** This word, or the adjective "RECOMMENDED," means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. **SHOULD NOT –** This phrase, or the phrase "NOT RECOMMENDED," means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. **MAY –** This word, or the adjective "OPTIONAL," means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product, whereas another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, although perhaps with reduced functionality. In the same vein an implementation that does include a particular option MUST be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature the option provides).

16 References

[1] RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", March 1999

[2] RFC 2119, "Key Words for Use in RFCs to Indicate Requirement Levels", March 1997

[3] RFC 2459, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", January 1999

[4] RFC 2560, "Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP", June 1999

[5] NCSA, "NCSA Certificate Policy," June 1999

[6] EuroPKI, "EuroPKI Certificate Policy version 1.1", October 2000