

Internet Draft	Randy Butler
Document: draft-gridforum-CP.txt	NCSA
Category: Informational	Tony J. Genovese
Expires April 2003	Esnet/LBNL
	October 2002

Global Grid Forum Certificate Policy Model

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This document describes a reference certificate policy for Certificate Authorities (CA) operating within the Global Grid Community (GGF). It is not a CP to be used for operating a CA in the GGF. This CP only addresses the use of X.509 certificates for authentication and explicitly avoided documenting policies for digital signature and encryption. The goal of this CP is help the GGF to deploy PKI to support technical inter-operation of our various Grid PKIs. This document is meant to serve as a model and is written at times as

if it were a policy to give readers an example. In many cases there are suggestions and alternatives that the reader will have to interpret on their own. The American Bar Association has produced a similar guidelines CP to help develop a generic CP [9]. This document will attempt to focus on issues relevant to the GGF.

Sections of this document that have the phrase "No Stipulation" reflect the community's best practice. It does not imply that a CA can not fill these sections in. It only means at this time the community has not specified any requirements.

Table of Contents

1.	Introduction	
1.1.	Overview.....	
1.2.	Identification.....	
1.3.	Community and applicability	
1.4.	Contact Details.....	
2.	General provisions.....	
2.1.	Obligations.....	
2.2.	Liability.....	
2.3.	Financial responsibility	
2.4.	Interpretation and Enforcement.....	
2.5.	Fees.....	
2.6.	Publication and Repository	
2.7.	Compliance audit.....	
2.8.	Confidentiality.....	
2.9.	Intellectual Property Rights	
3.	Identification and authentication	
3.1.	Initial Registration	
3.2.	Routine rekey.....	
3.3.	Rekey after revocation	
3.4.	Revocation request	
4.	Operational requirements.....	
4.1.	Certificate Application	
4.2.	Certificate Issuance	
4.3.	Certificate Acceptance	
4.4.	Certificate Suspension and Revocation.....	
4.5.	Security Audit Procedures	
4.6.	Records Archival.....	

4.7.	Key changeover
4.8.	Compromise and Disaster Recovery.....
4.9.	CA Termination.....
5.	Physical, procedural, and personnel security controls
5.1.	Physical Controls
5.2.	Procedural controls
5.3.	Personnel controls
6.	Technical security controls
6.1.	Key Pair Generation and Installation.....
7.	CA Certificates.....
7.1.	Private Key Protection
7.2.	Other aspects of key pair management.....
7.3.	Activation data
7.4.	Computer security controls
7.5.	Life cycle technical controls
7.6.	Network security controls
7.7.	Cryptographic module engineering controls
8.	Certificate and CRL profiles
8.1.	Certificate Profile
8.2.	CRL Profile.....
9.	Specification administration
9.1.	Specification change procedures.....
9.2.	Publication and notification policies
9.3.	CPS approval procedures
10.	References
	APPENDIX 1
	Appendix 2

1. Introduction

This CP was developed for the Global Grid community to reduce the cost and time needed to build a Grid PKI and increase policy and technical inter-operability in the Global Grid community. The Global Grid Forum is providing this CP as a reference Certificate Policy for all grids that wish to participate in the Global Grid Community. This document will not preclude local Grids from adding their own local CP to their Certificate's Certificate Policies Extension to specify specific local Grid requirements. This document is a compilation of

best practices and policy issues that will facilitate the deployment of PKI for GGF Grids.

The GGF will not run a PKI for the GGF community. This document's purpose is to bring together all current issues related to deploying a PKI in support of Grids. In this way it will facilitate anyone who wishes to deploy a PKI in that it provides technical guidance for policies that must be used by Grid PKIs. The document is written as if it were the certificate policy document for the general Grid forum however it is meant to provide guidance for those wishing to develop and document certificate policy for their Grid. It is expected that all PKIs deployed to support Grids will reference this document.

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

This Certificate Policy (CP) defines four certificate policies. The four policies represent four different assurance levels (Rudimentary, Basic, Medium, and High) for public key digital certificates. 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 there are some sections that are maintained for compatibility, although they do not apply exactly to the services offered by all grids. Appendix 1 provides a glossary of terms used in this document. It is mainly based on [1].

Within this document the words "MUST", "MUST NOT", "REQUIRED", "SHALL", "OPTIONAL" are to be interpreted as in RFC 2119 [2]. (See Appendix 2)

In this document the expression "conforming CA" is used to indicate a CA whose behavior is conforming to the set of provisions specified in this document.

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 which are not specified in this policy.

1.2. Identification

This is a GGF reference document and will not be assigned an OID, however it is recommended that each CP needs an OID assigned to it 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 CA has to take particular care when it has to decide if a certain organization or individual can manage a subject CA performing all the controls and checks detailed in this policy. A conforming CA MAY use as many RAs (registration authorities) 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 (RA) are useful for physical identification/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 CPS.

1.3.3. End entities

The end entities to be certified in accordance with this policy can be a natural person (individual or representing an organization) or a computer entity (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 a wide use of public-key certificates in many different

applications. In order 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 like HTTP, Telnet, FTP) SHOULD be supported. It's important to notice that this policy in principle doesn't want to put a priori limitation to 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 are established. However in order to evaluate if certificates issued in accordance with this policy are suitable for a certain application the chapter 2 about "General provisions" has to be read carefully and fully understood.

The certificate levels of assurance contained in this CP are set forth below, as well as examples of roles played by relevant personnel. In the Roles column, the numbers indicate the number of "people" or roles required (for power separation reasons) to stratify the assurance level.

Assurance Level	Risk	Roles
Rudimentary	Low	[1] Account Administration, Key Generation, Maintain Audit Logs, Archive, Performing Backups, Issuing and Revoking Certificates
Basic	Moderate	[1] Account Administration, Key Generation, Maintain Audit Logs and Archive, Performing Backups; [2] Issuing and Revoking Certificates
Medium	Moderate	[1] Account Administration, Key Generation; [2] Issuing and Revoking Certificates;

		[3] Maintain Audit Logs and Archive, Performing Backups
High	Significant	[1] Account Administration and Key Generation; [2] Maintain Audit Logs and Archives; [3] Issuing and Revoking Certificates; [4] Performing Backups

1.3.4.1 Rudimentary Assurance Level

This 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. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but 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, Maintain Audit Logs, Archive, perform backups, issuing and revoking certificates.

1.3.4.2 Basic Assurance Level

This level provides a basic 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 will be responsible for account administration, key generation, audit and archive configuration. The other role covers issuing and revoking 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

This 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, and 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 will be responsible for account administration, key generation, audit and archive configuration; a second role will be responsible for issuing and revoking certificates; and a third role will be responsible for maintaining the audit logs and archives.

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

This 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 will be responsible for account administration and key generation; a second role responsible for maintaining the audit logs and archives; a third role responsible for issuing and revoking certificates; and a fourth role responsible for performing backups.

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

1.4. Contact Details

1.4.1. Specification administration organization

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

1.4.2. Contact person

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

1.4.3. Person determining CPS suitability for the policy

It is the responsibility of conforming CAs have to establish their own a Policy Management Authority (PMA) that will oversee the CA. The PMA is responsible for setting policy, approving the CP and CPS, determination of compliance with the CPS, and oversight of activities related to the development and enforcement of policy as specified in the CP

2. General provisions

This chapter describes obligations for relevant parties and makes statements on liability, financial/economical issues. Moreover there's a section about confidentiality that classifies information into confidential information and publicly available and distributable information. Auditing statements are also located here.

2.1. Obligations

2.1.1. CA obligations

CAs are managed in general by a Policy Management Authority. If the CA has a PMA it is responsible to insure the CA obligations listed.

Certificate Authorities are responsible for all aspects of the issuance and management of a certificate referencing this Policy, including

- * 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/enrollment process,
- * Verification of the identity of the applicant,
- * Certificate creation process,
- * 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.
- * Define and publish a dispute resolution procedure,
- * Publish CA audit results
- *

By issuing a certificate that references this Certificate Policy, the CA certifies 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, that:

- * The CA has issued, and will manage, the certificate in accordance with this Policy,
- * There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS, and
- * 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 versus the CA
- * adhere to the agreement made with the CA

2.1.3. Subscriber obligations

In all cases, subscribers will be 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, and
- * 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 if:

- * The relying party is familiar with the CPS of the CA that generated the certificate, and 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, and
- * 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 (CRLs).

The repository should be available 7X24.

2.2. Liability

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.

Conforming CA MAY accept liability. Considering that this policy is primarily established to promote the adoption of certificates as a mean to increase computer and network security in a broad variety of applications, the subsection 1.3.4 states that there is no a priori limitation to applicability of certificates issued in accordance with this policy. If no limitation is put on certificate applicability, this policy suggests that CA liability will be 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 CA's

private key. In every case the complete list of accepted liabilities MUST be specified in the CPS.

2.2.2. RA liability

Cf. subsection 2.2.1

2.3. Financial responsibility

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

2.3.1. Indemnification by relying parties

Must be defined in the CP and CPS

2.3.2. Fiduciary relationships

Must be defined in the CP and CPS

2.3.3. Administrative processes

Must be defined in the CP and CPS

2.4. Interpretation and Enforcement

2.4.1. Governing law

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

2.4.2. Severability, survival, merger, notice

In the event that the CA ceases operation, all subscribers, sponsoring organizations, RAs, RSPs, and Qualified Relying Parties will be promptly notified of the termination.

In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination.

2.4.3. Dispute resolution procedures

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

2.5. Fees

2.5.1. Certificate issuance or renewal fees

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

2.5.2. Certificate access fees

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

2.5.3. Revocation or status information access fees

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

2.5.4. Fees for other services i.e. policy information

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

2.5.5. Refund policy

Must be defined in the CP and CPS

2.6. Publication and Repository

2.6.1. Publication of CA information

Each Authorized CA shall operate a secure on-line repository that is available to Qualified Relying Parties and that contains:

- * * Audit results
- * * Certificates issued that reference this Policy,
- * * Signed Certificate Revocation List (CRL) 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 SHALL 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, and
- * * Other relevant information relating to certificates that reference this Policy.
- *

2.6.2. Frequency of publication

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

2.6.3. 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 like e-mail addresses or when CA decides to charge fees for certification services).

2.6.4. Repositories

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

2.7. Compliance audit

To develop trust in the CA, relying organizations usually require an audit of the facilities and operations of the CA to insure 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 DOEGrids used to evaluate its member organizations. Third party audits were considered too expensive for the level of trust that was required.

2.7.1. Frequency of entity compliance audit

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

2.7.2. Identity/qualifications of auditor

The team will be comprised of members representing applications, infrastructure, and policy/management activities not affiliated with the CA or the organization that manages the CA.

2.7.3. 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.

2.7.4. Topics covered by audit

The audit will verify the quality of the services provided by the CA, that the CA complies with all of the requirements of this Policy and its CPS, and that the CPS CP and CPS is consistent with the requirements of this Policy.

2.7.5. Actions taken as a result of deficiency

If a CA fails an audit, organizations or relying parties should consider what they want to do. 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.

2.7.6. Communication of results

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.

2.8. Confidentiality

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

2.8.1. Types of information to be kept confidential

All subscribers' information that is not present in the certificate and 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.

2.8.2. Types of information not considered confidential

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

2.8.3. Disclosure of certificate revocation/suspension information

When a certificate is revoked/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.

2.8.4. 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 that exhibit regular warrant.

2.8.5. Release as part of civil discovery

Must be defined in the CP and CPS.

2.8.6. 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.

2.8.7. Other information release circumstances

Must be defined in the CP and CPS.

2.9. Intellectual Property Rights

A conforming CA MUST NOT claim any IPR on issued certificates.

3. Identification and authentication

This component 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. This component also addresses naming practices, including name ownership recognition and name dispute resolution.

3.1. Initial Registration

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 fields of the certificate Global Grid Forum policy is conforming to RFC 2459 [3]. Conforming CA MUST detail in the CP and CPS the types and format of names used.

3.1.2. Need for names to be meaningful

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

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

3.1.3. Rules for interpreting various name forms

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 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 resolution procedure

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

3.1.6. Recognition, authentication and role of trademarks

Must be defined in the CP and CPS.

3.1.7. Method to prove possession of private key

The adoption of proper method to prove possession of the private key corresponding to the public key being certified is required.

The method adopted MUST be detailed in the CP and CPS. Conforming CA MUST NOT issue certificate for which the proof of possession fails. This policy discourages generation of private key done by 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, issuing CA MUST have evidence that the organization has complete knowledge about this fact. In order to obtain this result issuing CA MUST require some documents. In all cases suitable legal documents that prove the data to be certified MUST be presented by means of out-of-band methods. 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 mean to guarantee strong cryptographic authentication of communicating entities. Bearing in mind this premise GGF believes that authentication of individual identity is REQUIRED. The RECOMMENDED method of authentication requires that individual to present personally to the authenticating CA or RA suitable identification documents. Other methods like videoconference MAY be adopted. If the subject to be

certified is a software component the person who submits the request MUST prove that he has the necessary authorization (The exact 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 and/or RAs shall ensure that the applicant's identity information and public key are bound adequately. Additionally, CAs and/or RAs shall record the process that was followed for issuance of each certificate. Process information shall depend upon 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 rudimentary:

- * * 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 USA CPs and may not be applicable to other countries. Every CP needs to comply with the local privacy and an identity law of the country 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 via correspondence.

No proofing 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, it shall contain an Alternative Subject Name that is populated and marked as non-critical. This level is intended only for ensuring data integrity checking.

NB: 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), but if the latter 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 using a protocol defined in the Certification Practice Statement (CPS) 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 (CPS). 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 (RA), a Trusted Agent approved by the RA as being authorized to confirm identities (such as Public Notaries), that uses a stamp, seal or other mechanism to confirm that it has authenticated the identity of the applicant.

NB: Some countries do not provide Government issued Identifications. Other strong local methods will need to be defined.

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 (such as comparison of biometric data to identities pre-verified to the standards of this CP, obtained via authenticated interaction with secured databases) may be used.

The Registration Authority or its designated representative shall personally verify the applicant's identity; or the applicant shall provide credential information, which required an antecedent 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 marked as non-critical.

When private keys are delivered to Subscribers via hardware tokens, the Subscriber shall personally appear before the RA or Trusted Agent to obtain his or her 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, 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 (CPS). The certificate shall contain an X.500 Distinguished Name, and optional Alternative Subject Name if marked non-critical.

High: The applicant shall appear in person before the Registration Authority (RA), or a Trusted Agent approved by the RA.

NB: Some countries do not provide Government issued Identifications. Other strong local methods will need to be defined.

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 (such as comparison of biometric data to identities pre-verified to the standards of this CP, obtained via authenticated interaction with secured databases) may be used.

When private keys are delivered to Subscribers via hardware tokens, the Subscriber shall personally appear before the RA or Trusted Agent to obtain his or her token or token activation data.

The private key corresponding to the public key offered for the certificate shall exist in 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 (CPS). The certificate shall contain an X.500 Distinguished Name,

and optional Alternative Subject Name if marked non-critical.

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.

The table below summarizes the identification requirements for each level of assurance.

Assurance Level	Identification Requirements
Rudimentary	<ul style="list-style-type: none">• No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address
Basic	<ul style="list-style-type: none">• Identity may be established by in-person appearance before a Registration Authority or designated representative; or 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. NB: Some countries do not provide Government issued Identifications. Other strong local methods will need to be defined. <ul style="list-style-type: none">• Credentials required are either 1 Government-issued Picture I.D., or two Non-Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
High	Identity established by in-person appearance before the Registration

	<p>Authority or Trusted Agent. NB: Some countries do not provide Government issued Identifications. Other strong local methods will need to be defined.</p> <ul style="list-style-type: none"> • Credentials required are either 1 Government-issued Picture I.D., or two Non-Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
--	---

3.2. Routine rekey

This policy doesn't mandate any compulsory rekey. After certificate expiration, the CA MAY issue a new certificate both 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 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.

Assurance Level	Routine Rekey Requirements for End-Entity Subscriber Signature and Encryption Certificates
Rudimentary	<p>Re-key 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</p> <p>Identity may be established through use of current signature key</p>
Basic	<p>Re-key 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</p> <p>Identity may be established through use of</p>

Assurance Level	Routine Rekey Requirements for End-Entity Subscriber Signature and Encryption Certificates
	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	Re-key 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	Re-key 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 re-certified. The public key MAY be re-certified if the revocation is only 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 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. 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 PIN (Personal Identification Number). The exact procedures supported MUST be detailed in the CP and CPS. See section 4.4.2

4. Operational requirements

This component is used to specify requirements imposed upon entities involved in the certification and certificate revocation process.

4.1. Certificate Application

This policy permits two alternatives 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 submit 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 the authentication accomplished by methods specified in section 3.1, CA SHOULD issue the certificate. In the case of issuance CA MUST notify the requester. If for any reasons CA decides not to issue the certificate (even if the checks and the authentication were correct) it SHOULD notify the reason for this choice to the requester.

4.3. Certificate Acceptance

No stipulation.

4.4. Certificate Suspension and Revocation

Conforming CA is responsible for issuing CRLs and for publishing signed versions. Although [3] doesn't require CAs to issue CRLs, 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. This includes situations where:

- * * 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. Who can request revocation

Conforming CA MUST accept a revocation request made by the holder of the certificate to be revoked. Moreover the revocation request MAY come from the CA that issued the certificate or from 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. 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 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/CRLs issued using the compromised private key.
- *

4.4.4. Revocation request grace period

The conforming CA decides: what is 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 conforming CA are not required to offer the suspension service. Information on public keys of disabled users MAY be available from CA repository.

4.4.6. Who can request suspension

In the case that a CA offers the suspension service, 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. 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 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 (if applicable)

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

4.4.10. CRL checking requirements

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/status checking
availability

Conforming CA MAY support on-line revocation/status checking. Bearing in mind that this policy requires conforming CA to issue CRL, it isn't mandatory to implement on-line revocation/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
available

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 type of events that are recorded for archival purposes from 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

Conforming CA SHOULD archive:

- * * 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 RA The RAs SHOULD archive
- * * All validation information collected from the subscriber
- * * All relevant messages exchanged with CA
- *

4.6.2. Retention period for archive

The minimum retention period is 2 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 be compromised, the CA MUST at least:
 - * * 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 be 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 be 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 a natural or other type of disaster

No stipulation

4.9. CA Termination

Termination of a CA is regarded as the situation where 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

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 exposures

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 like 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 person required per task

No stipulation

5.2.3. Identification and authentication for each role

No stipulation

5.3. Personnel controls

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

1

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

6.1. Key Pair Generation and Installation

This component is used to define the provisions for key management and the corresponding technical security controls.

6.1.1. Key pair generation

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.

6.1.2. Private key delivery to entity

The entity MAY generate his/her own key pair. It is important to notice that in the case of key pair generation done by CA, the key pair MUST be given to the end entity in a secure way. Further details MUST be specified in the CP and CPS.

6.1.3. Public key delivery to certificate issuer

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

6.1.4. CA public key delivery to users

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 CA's public keys MUST be publicly available in a repository accessible via standard protocol such as HTTP or LDAP.

6.1.5. Key sizes

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 length values 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.

6.1.6. Public key parameters generation

No stipulation

6.1.7. Parameter quality checking

No stipulation

6.1.8. Hardware/software key generation

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

6.1.9. Key usage purposes (as per X.509 v3 key usage field)

A CA through the KeyUsage extension in the certificate MAY restrict the purposes for which a key can be used. This is a field that 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. This means that the certificate MUST be used only for a purpose for which the corresponding key usage bit is set to one.

7. CA Certificates

In CA's certificates KeyUsage extension MUST be specified in the CP/CPS.

7.1. Private Key Protection

7.1.1. Standards for cryptographic module

This policy doesn't mandate the adoption of cryptographic module compliant with pre-determined 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 (n out of m) multi-person control

The private key of individual MUST NOT be under (n out of m) multi-person 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 CA.

7.1.4. Private key backup

This policy suggests that 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 archival

This policy suggests the implementation of a procedure for private key archival 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 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. Method of activating private key

Specific details about how to activate private key SHOULD be found in the CP and CPS. As a general suggestion this policy recommends that 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 passphrase, 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. Method of deactivating private key

No stipulation

7.1.9. Method of destroying private key

No stipulation

7.2. Other aspects of key pair management

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 the public and private keys

No stipulation

7.3. Activation data

7.3.1. Activation data generation and installation

Pass phrases or PINs MUST be selected according to "best practice". This means that it is necessary to suggest a suitable minimal length for the pass phrases and to enforce mechanisms 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, etc). 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

7.4.1. Specific computer security technical requirements

No stipulation

7.4.2. Computer security rating

No stipulation

7.5. 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

This policy strongly suggests that 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 in an appropriate way from disclosure.

7.7. Cryptographic module engineering controls

No stipulation

8. Certificate and CRL profiles

8.1. Certificate Profile

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

8.2. CRL Profile

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. Specification administration

9.1. Specification change procedures

Editorial changes can be made to the policy and CPS. In case of substantial changes of 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 notified 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

Conforming CA MUST be evaluated for compliance with the policy. In order to obtain CPS approval conforming CAs MAY submit their CPS to the contact people specified in section 1.4.3 which describes the PMA After that conforming CA MUST wait for the answer. The time limit for completing the evaluation is established in 60 days. It might be acceptable to have CA self certification for compliance, but in this case if non-compliance is reported to Global Grid Forum organization then the CA certificate will be revoked.

10. 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
- [7] Federal Bridge Certificate Authority "X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 1.9", May 27, 2000
- [8] INFN CA "Certificate Policy and Certification Practice Statement version 0.3 (Draft)", March 2001
- [9] Section of Science and Technology Law - American Bar Association, Information Security Committee: PKI

APPENDIX 1

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. It is important to note that 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 and/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 which, 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, which a certification authority employs in issuing, certificates.

Certificate revocation list (CRL) - A CRL is 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) - In the context of a particular certificate, the issuing CA is the CA that issued 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 which 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). [Note: 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 and/or 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

Appendix 2

Key words for use in RFCs to Indicate Requirement Levels

According to RFC 2119 [2] "Key words for use in RFCs to Indicate Requirement Levels", we specify how the main keywords used in RFCs should be interpreted. Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHAL 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", mean that the definition is an absolute prohibition of the specification.
3. **SHOULD** This word, or the adjective "RECOMMENDED", mean 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" mean 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", mean 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 while another vendor may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)