



Category: CP/CPS

Status: published

Document: PK Grid Certification Authority
Certificate Policy and Certificate Practice
Statement

Editors: Adeel-ur-Rehman, Mansoor-ul-Islam
Sheikh, Manzoor Ahmad

Number of pages: 48

PK GRID Certificate Authority CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

Document OID: 1.3.6.1.4.1.19323.1.1.3.3

Prepared By:

National Centre for Physics (NCP),
Quaid-i-Azam University Campus,
Shahdra Valley Road, Islamabad,
Pakistan

Ph: (+ 92 - 51) 207 7300

Fax: (+92 - 51) 207 7393

URL: <http://www.ncp.edu.pk>

1. Introduction.....	8
1.1 OVERVIEW	8
1.2 DOCUMENT NAME AND IDENTIFICATION	8
1.3 PKI PARTICIPANTS	8
1.3.1 Certification Authorities	8
1.3.2 Registration Authorities	8
1.3.3 Subscribers	8
1.3.4 Relying Parties	8
1.3.5 Other Participants	9
1.4 CERTIFICATE USAGE	9
1.4.1 Appropriate Certificate Uses.....	9
1.4.2 Prohibited Certificate Uses	9
1.5 POLICY ADMINISTRATION	9
1.5.1 Organization Administering the Document.....	9
1.5.2 Contact Person	9
1.5.3 Person Determining CPS Suitability for the Policy	10
1.5.4 CPS Approval Procedures.....	10
1.6 DEFINITIONS AND ACRONYMS	10
2. Publication and Repository Responsibilities.....	13
2.1 REPOSITORIES	13
2.2 PUBLICATION OF CERTIFICATION INFORMATION.....	13
2.3 TIME OR FREQUENCY OF PUBLICATION	13
2.4 ACCESS CONTROL ON REPOSITORIES.....	13
3. Identification and Authentication	15
3.1 NAMING.....	15
3.1.1 Types of Names	15
3.1.2 Need for Names to be Meaningful	15
3.1.3 Anonymity or Pseudonymity of Subscribers	15
3.1.4 Rules for Interpreting Various Name Forms	15
3.1.5 Uniqueness of Names.....	15
3.1.6 Recognition, Authentication, and Role of Trademarks.....	15
3.2 INITIAL IDENTITY VALIDATION	16
3.2.1 Method to Prove Possession of Key.....	16
3.2.2 Authentication of Organization Identity.....	16
3.2.3 Authentication of Individual Identity.....	16
3.2.3.1 Person Requesting a Certificate	16
3.2.3.2 Host certificate	16
3.2.4 Non-verified Subscriber Information.....	16
3.2.5 Validation of Authority	16
3.2.6 Criteria of Interoperation.....	17
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	17
3.3.1 Identification and authentication for Routine re-key.....	17
3.3.2 Identification and authentication for re-key after revocation	17
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	17
4. Certificate Life-cycle Operational Requirements	18
4.1 CERTIFICATE APPLICATION	18
4.1.1 Who can submit a Certificate Application	18
4.1.2 Enrollment Process and Responsibilities	18
4.2 CERTIFICATE APPLICATION PROCESSING	18
4.2.1 Performing Identification and Authentication Functions	18
4.2.2 Approval or Rejection of Certificate Applications.....	19
4.2.3 Time to Process Certificate Applications	19

4.3	CERTIFICATE ISSUANCE.....	19
4.3.1	CA Actions during Certificate Issuance.....	19
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate.....	19
4.4	CERTIFICATE ACCEPTANCE.....	20
4.4.1	Conduct Constituting Certificate Acceptance.....	20
4.4.2	Publication of the Certificate by the CA.....	20
4.4.3	Notification of Certificate Issuance by the CA to other Entities.....	20
4.5	KEY PAIR AND CERTIFICATE USAGE.....	20
4.5.1	Subscriber Private Key and Certificate Usage.....	20
4.5.2	Relying Party Public Key and Certificate Usage.....	20
4.6	CERTIFICATE RENEWAL.....	21
4.6.1	Circumstances for Certificate Renewal.....	21
4.6.2	Who May Request Renewal.....	21
4.6.3	Processing Certificate Renewal Requests.....	21
4.6.4	Notification of New Certificate Issuance to Subscriber.....	21
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	21
4.6.6	Publication of the Renewal Certificate by the CA.....	21
4.6.7	Notification of Certificate Issuance by the CA to other Entities.....	21
4.7	CERTIFICATE RE-KEY.....	21
4.7.1	Circumstance for Certificate Re-key.....	21
4.7.2	Who May Request Certification of a New Public Key.....	22
4.7.3	Processing Certificate Re-keying Requests.....	22
4.7.4	Notification of new Certificate Issuance to Subscriber.....	22
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate.....	22
4.7.6	Publication of the Re-keyed Certificate by the CA.....	22
4.7.7	Notification of Certificate Issuance by the CA to other Entities.....	22
4.8	CERTIFICATE MODIFICATION.....	22
4.8.1	Circumstances for Certificate Modification.....	22
4.8.2	Who May Request Certificate Modification.....	23
4.8.3	Processing Certificate Modification Requests.....	23
4.8.4	Notification of New Certificate Issuance to Subscriber.....	23
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	23
4.8.6	Publication of the Modified Certificate by the CA.....	23
4.8.7	Notification of Certificate Issuance by the CA to Other Entities.....	23
4.9	CERTIFICATE REVOCATION AND SUSPENSION.....	23
4.9.1	Circumstances for Revocation.....	23
4.9.2	Who Can Request Revocation.....	24
4.9.3	Procedure for Revocation Request.....	24
4.9.4	Revocation Request Grace Period.....	24
4.9.5	Time within which CA must Process the Revocation Request.....	24
4.9.6	Revocation Checking Requirement for Relying Parties.....	24
4.9.7	CRL Issuance Frequency.....	24
4.9.8	Maximum Latency for CRLs.....	24
4.9.9	On-line Revocation/Status Checking Availability.....	25
4.9.10	On-line Revocation Checking Requirements.....	25
4.9.11	Other Forms of Revocation Advertisements Available.....	25
4.9.12	Special Requirements Re-key Compromise.....	25
4.9.13	Circumstances for Suspension.....	25
4.9.14	Who can Request Suspension.....	25
4.9.15	Procedure for Suspension Request.....	25
4.9.16	Limits on Suspension Period.....	25
4.10	CERTIFICATE STATUS SERVICES.....	25
4.10.1	Operational Characteristics.....	25

4.10.2 Service Availability.....	26
4.10.3 Optional Features	26
4.11 END OF SUBSCRIPTION.....	26
4.12 KEY ESCROW AND RECOVERY	26
4.12.1 Key Escrow and Recovery Policy and Practices	26
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	26
5. Facility, Management and Operational Controls	27
5.1 PHYSICAL CONTROLS	27
5.1.1 Site Location and Construction	27
5.1.2 Physical Access	27
5.1.3 Power and Air Conditioning	27
5.1.4 Water Exposures	27
5.1.5 Fire Prevention and Protection.....	27
5.1.6 Media Storage	27
5.1.7 Waste Disposal	28
5.1.8 Off-site backup	28
5.2 PROCEDURAL CONTROLS	28
5.2.1 Trusted Roles	28
5.2.2 Number of Persons Required per Task	28
5.2.3 Identification and Authentication for Each Role	28
5.2.4 Roles Requiring Separation of Duties	28
5.3 PERSONNEL CONTROLS	28
5.3.1 Qualifications, Experience, and Clearance Requirements	28
5.3.2 Background Check Procedures.....	28
5.3.3 Training Requirements	29
5.3.4 Retraining Frequency and Requirements	29
5.3.5 Job Rotation Frequency and Sequence.....	29
5.3.6 Sanctions for Unauthorized Actions	29
5.3.7 Independent Contractor Requirements	29
5.3.8 Documentation Supplied to Personnel.....	29
5.4 AUDIT LOGGING PROCEDURES	29
5.4.1 Types of Events Recorded.....	29
5.4.2 Frequency of Processing Log	29
5.4.3 Retention Period for Audit Log.....	30
5.4.4 Protection of Audit Log.....	30
5.4.5 Audit Log Backup Procedures	30
5.4.6 Audit Collection System (internal vs. external)	30
5.4.7 Notification to Event-causing Subject	30
5.4.8 Vulnerability assessments.....	30
5.5 RECORDS ARCHIVAL.....	30
5.5.1 Types of records archived	30
5.5.2 Retention Period for Archive.....	30
5.5.3 Protection of Archive.....	31
5.5.4 Archive Backup Procedures	31
5.5.5 Requirements for Time-stamping of Records	31
5.5.6 Archive Collection System (internal or external).....	31
5.5.7 Procedures to Obtain and Verify Archive Information	31
5.6 KEY CHANGEOVER.....	31
5.7 COMPROMISE AND DISASTER RECOVERY	31
5.7.1 Incident and Compromise Handling Procedures.....	31
5.7.2 Computing Resources, Software, and/or Data are corrupted	32
5.7.3 Entity Private Key Compromise Procedures	32
5.7.4 Business Continuity Capabilities after a Disaster	32

5.8 CA or RA TERMINATION	32
6. Technical Security Controls	33
6.1 KEY PAIR GENERATION AND INSTALLATION.....	33
6.1.1 Key Pair Generation	33
6.1.2 Private Key Delivery to Subscriber	33
6.1.3 Public Key Delivery to Certificate Issuer.....	33
6.1.4 CA Public Key Delivery to Relying Parties	33
6.1.5 Key sizes	33
6.1.6 Public Key Parameters Generation and Quality Checking	33
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)	33
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	34
6.2.1 Cryptographic Module Standards and Controls	34
6.2.2 Private Key (n out of m) Multi-person Control.....	34
6.2.3 Private Key Escrow	34
6.2.4 Private Key Backup.....	34
6.2.5 Private Key Archival.....	34
6.2.6 Private Key Transfer into or from a Cryptographic Module	34
6.2.7 Private Key Storage on Cryptographic Module.....	34
6.2.8 Method of Activating Private Key	34
6.2.9 Method of Deactivating Private Key.....	35
6.2.10 Method of Destroying Private Key	35
6.2.11 Cryptographic Module Rating.....	35
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT	35
6.3.1 Public Key Archival	35
6.3.2 Certificate Operational Periods and Key Pair Usage Periods.....	35
6.4 ACTIVATION DATA	35
6.4.1 Activation Data Generation and Installation.....	35
6.4.2 Activation Data Protection	35
6.4.3 Other Aspects of Activation Data	36
6.5 COMPUTER SECURITY CONTROLS	36
6.5.1 Specific Computer Security Technical Requirements	36
6.5.2 Computer Security Rating.....	36
6.6 LIFE CYCLE TECHNICAL CONTROLS.....	36
6.6.1 System Development Controls	36
6.6.2 Security Management Controls.....	36
6.6.3 Life Cycle Security Controls.....	36
6.7 Network Security Controls	36
6.8 TIME-STAMPING	36
7. Certificate, CRL and OCSP Profiles	37
7.1 CERTIFICATE PROFILE	37
7.1.1 Version Number(s)	37
7.1.2 Certificate Extensions	37
7.1.3 Algorithm Object Identifiers	38
7.1.4 Name Forms.....	38
7.1.5 Name Constraints.....	38
7.1.6 Certificate Policy Object Identifier	38
7.1.7 Usage of Policy Constraints extension.....	39
7.1.8 Policy Qualifiers Syntax and Semantics.....	39
7.1.9 Processing Semantics for the Critical Certificate Policies Extension.....	39
7.2 CRL PROFILE	39
7.2.1 Version Number(s)	39

7.2.2 CRL and CRL Entry Extensions.....	39
7.3 OSCP PROFILE	39
7.3.1 Version Number(s)	39
7.3.2 OSCP Extensions	39
8. Compliance, Audit and other Assessments	40
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	40
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR	40
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	40
8.4 TOPICS COVERED BY ASSESSMENT	40
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	40
8.6 COMMUNICATION OF RESULTS	40
9. Other Business and Legal Matters	41
9.1 FEES	41
9.1.1 Certificate Issuance or Renewal Fees.....	41
9.1.2 Certificate Access Fees	41
9.1.3 Revocation or Status Information Access Fees	41
9.1.4 Fees for Other Services	41
9.1.5 Refund Policy.....	41
9.2 FINANCIAL RESPONSIBILITY.....	41
9.2.1 Insurance Coverage.....	41
9.2.2 Other Assets.....	41
9.2.3 Insurance or Warranty Coverage for End-entities	41
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION.....	42
9.3.1 Scope of Confidential Information	42
9.3.2 Information not within the Scope of Confidential Information.....	42
9.3.3 Responsibility to Protect Confidential Information.....	42
9.4 PRIVACY OF PERSONAL INFORMATION.....	42
9.4.1 Privacy Plan.....	42
9.4.2 Information Treated as Private	42
9.4.3 Information not Deemed Private	42
9.4.4 Responsibility to Protect Private Information	42
9.4.5 Notice and Consent to Use Private Information	43
9.4.6 Disclosure Pursuant to Judicial or Administrative Process	43
9.4.7 Other Information Disclosure Circumstances	43
9.5 INTELLECTUAL PROPERTY RIGHTS.....	43
9.6 REPRESENTATIONS AND WARRANTIES.....	43
9.6.2 RA Representations and Warranties	43
9.6.3 Subscriber Representations and Warranties.....	43
9.6.4 Relying Party Representations and Warranties	44
9.6.5 Representations and Warranties of Other Participants	44
9.7 DISCLAIMERS OF WARRANTIES	44
9.8 LIMITATIONS OF LIABILITY	44
9.9 INDEMNITIES	44
9.10 TERM AND TERMINATION	44
9.10.1 Term	44
9.10.2 Termination	45
9.10.3 Effect of Termination and Survival.....	45
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	45
9.12 AMENDMENTS.....	45
9.12.1 Procedure for Amendment	45
9.12.2 Notification Mechanism and Period	45
9.12.3 Circumstances under which OID must be changed.....	45

9.13 DISPUTE RESOLUTION PROVISIONS	45
9.14 GOVERNING LAW	45
9.15 COMPLIANCE WITH APPLICABLE LAW	46
9.16 MISCELLANEOUS PROVISIONS	46
9.16.1 Entire agreement.....	46
9.16.2 Assignment	46
9.16.3 Severability	46
9.16.4 Enforcement (attorneys' fees and waiver of rights)	46
9.16.5 Force Majeure	46
9.17 OTHER PROVISIONS	46
APPENDIX – A	47
APPENDIX – B	48

1. Introduction

1.1 OVERVIEW

This document is based on the structure suggested by the RFC 3647. It defines the Certificate Policy and the Certification Practice Statement of the PK-GRID (Pakistan Grid) Certification Authority (CA) and specifies the actual policies, practices, and obligations for the issuance and management of certificates. PK-GRID-CA operations are managed entirely by National Centre for Physics (NCP), Islamabad. Terms used in this document are explained in Definitions and Acronyms.

1.2 DOCUMENT NAME AND IDENTIFICATION

- Document Title: '**PK-GRID-CA Certificate Policy and Certification Practice Statement**'
- Document O.I.D.: 1.3.6.1.4.1.19323.1.1.3.3
- Document Date: January 2016
- Expiration: This document is valid until further notice

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

PK-GRID-CA does not issue certificates to subordinate certification authorities.

1.3.2 Registration Authorities

The PK-GRID-CA manages the functions of its Registration Authorities. Unlike before, currently, only NCP itself is acting as the RA of PK-GRID-CA due to having small user community.

New registration authorities may be created by the PK-GRID-CA as required. Existing Registration Authorities will be automatically removed if they do not remain NCP working partners.

1.3.3 Subscribers

The PK-GRID-CA will issue certificates to entities, which are based and/or having offices in Pakistan, and are intended for cross-organizational sharing of resources. The focus of these organizations should also be in research and/or education.

1.3.4 Relying Parties

Users/Hosts of GRID computing infrastructure, that are using the public keys of certificates issued by the PK-GRID-CA for signature verification and/or encryption, will be considered as relying parties.

1.3.5 Other Participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Certificates issued by the PK-GRID-CA may be used for applications suitable for X.509 certificates, e.g. Email signing and encryption, authentication and encryption of communications, authentication of users, hosts and services etc.

1.4.2 Prohibited Certificate Uses

The use of certificates for financial transactions or long-term encryption of data is strictly forbidden. Any other use notwithstanding the above is explicitly prohibited.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

National Centre for Physics (NCP), Islamabad is administering the PK-GRID-CA.
The PK-GRID-CA Address for operational issues is:

PK-GRID Certification Authority

IT Department
National Centre for Physics
Quaid-i-Azam University Campus
Shahdra Valley Road
Islamabad - 44000
Pakistan
Phone: (+92 - 51) 207 7300
Fax: (+ 92 - 51) 207 7393
Email: pkgrid-ca@ncp.edu.pk

1.5.2 Contact Person

The contact person for questions related with this document and PK-GRID-CA operations is:

Adeel ur Rehman

IT Department

National Centre for Physics
Quaid-i-Azam University Campus
Shahdra Valley Road
Islamabad - 44000
Pakistan
Phone: (+92 - 51) 207 7300 (Ext: 319)
Fax: (+ 92 - 51) 207 7393
Email: adeel.rehman@ncp.edu.pk

1.5.3 Person Determining CPS Suitability for the Policy

The person determining the CPS suitability for the policy is:

Mansoor ul Islam Sheikh
IT Department
National Centre for Physics
Quaid-i-Azam University Campus
Shahdra Valley Road
Islamabad - 44000
Pakistan
Phone: (+92 - 51) 207 7300 (Ext : 332)
Fax: (+ 92 - 51) 207 7393
Email: mansoor.sheikh@ncp.edu.pk

1.5.4 CPS Approval Procedures

The CPS is approved by the NCP Management running the PK-GRID-CA operations, which is then submitted to EU-Grid-PMA (European Grid Policy Management Authority) for acceptance and accreditation.

1.6 DEFINITIONS AND ACRONYMS

Activation Data

Data values, other than keys that are required to operate cryptographic modules. These are needed to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

Certification Authority (CA)

The entity/system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA).

Certificates – or Public Key Certificates

A data structure containing the public key of an end entity and some other information is digitally signed with the private key of the CA that issued it.

Certificate Policy (CP)

A named set of rules 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 Practice Statement (CPS)

A statement of the practices, a CA employs in issuing certificates.

Certificate Revocation Lists (CRL)

A CRL is a time stamped list identifying revoked certificates that is signed by a CA and made freely available in a public repository.

End Entity

A certificate subject that does not sign certificates (i.e., personal and host certificates).

Host Certificate

A certificate used for server authentication and encryption of communications. It will represent a single machine.

Public Key Infrastructure (PKI)

A term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. All of this implies a set of standards for applications that use encryption.

Personal Certificate

A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Qualifier

The policy-dependent information accompanies a certificate policy identifier in an X.509 certificate.

Private Key

In a PKI, a cryptographic key created and kept private by a subscriber. It may be used to make digital signatures which may be verified by the corresponding public key; to decrypt the message encrypted by the corresponding public key; or, with other information, to compute a piece of common shared secret information.

Public Key

In a PKI, a cryptographic key created and made public by a subscriber. It may be used to encrypt information that may be decrypted by the corresponding private key; or to verify the digital signature made by the corresponding private key.

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).

Relying Party

Any entity relying on a certificate, certificate revocation list, certificate chain, this Certification Practice Statement, Certificate Policies or any other information published by the CA.

SHA

SHA stands for Secure Hash Algorithm. Hash algorithms compute a fixed-length digital representation (known as a *message digest*) of an input data sequence (the *message*) of any length. They are called “secure” when, “it is computationally infeasible to:

- Find a message that corresponds to a given message digest, or
- Find two different messages that produce the same message digest.

SHA1 is a superior version of its first implementation i.e. SHA0. It was considered to be the successor to MD5 (Message Digest), an earlier, widely-used hash function.

As now, SHA1 is getting weaker, SHA-2 is being replaced by it and is considered to be the standard hash algorithm from now onwards.

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

Subscriber

In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.

SSL

Secure Socket Layer is a protocol that transmits our communications over the network in an encrypted form and ensures that the information is sent unchanged, only to the computer we intended to send it to.

2. Publication and Repository Responsibilities

2.1 REPOSITORIES

All the on-line and the off-line repositories of the PK-GRID-CA are operated by the National Centre for Physics.

The online repository is published at the URL <https://www.ncp.edu.pk/pk-grid-ca>. The repository is run at least on a best-effort basis.

The address for issues regarding the repositories is:

PK-GRID Certification Authority
National Centre for Physics
Quaid-i-Azam University Campus
Shahdra Valley Road
Islamabad - 44000
Pakistan
Phone: (+92 – 51) 207 7300
Fax: (+92 – 51) 207 7393
E-mail: pkgrid-ca@ncp.edu.pk

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The PK-GRID-CA operates on-line repositories that contain:

- The PK-GRID-CA root certificate.
- Issued host and user certificates that reference this or any old policy.
- The latest Certificate Revocation List (CRL).
- A copy of documents, which specifies the CP, CPS and old policies.
- The official contact e-mail address and physical contact address.
- Other relevant information.

The online repositories are published at the following URL:

<https://www.ncp.edu.pk/pk-grid-ca>

All valid certificates are published at the following URL:

<https://www.ncp.edu.pk/pk-grid-ca/validcerts.php>

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates will be published as soon as they are issued. CRLs will be published as soon as issued or at least after every twenty-three (23) days. New versions of CP-CPS will be published as soon as they have been approved.

2.4 ACCESS CONTROL ON REPOSITORIES

- PK-GRID-CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS.

- The PK-GRID-CA web site is maintained on a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available on a 24 hours a day, 7 days a week basis.
- All foreseen/scheduled downtimes in the repository shall be announced to PMA and as widely as possible.

3. Identification and Authentication

3.1 NAMING

3.1.1 Types of Names

The subject names for the certificate applicants shall follow the X.509 standard:

- In case of personal certificate the subject name must include the person's full name.
- In case of host/server certificate the subject name must include the FQDN of the host/server.

3.1.2 Need for Names to be Meaningful

The subject name must represent the subscriber in a way that is easily understandable by humans and must have a reasonable association with the authenticated name of the subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

PK-GRID-CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

- Each entity has a clear and unique Distinguished Name in the certificate subject field.
- Any name under this CP-CPS will have "C=PK, O=NCP".
- For a user certificate the common name (CN) name must be the full name of the subscriber.
- In case the subscriber is a host or service the subject/common name must be the FQDN of the host/server.

3.1.5 Uniqueness of Names

The name listed in a certificate shall be unambiguous and unique for all certificates issued by the PK-GRID-CA. If the name presented by the subscriber is not unique, additional numbers or letters may be appended to the name to ensure uniqueness. Certificates must apply to unique individuals or resources. Users must not share certificates.

If a user drops out of the rekey chain, the DN issued to him is not reused or issued to any other individual.

PK-GRID-CA will not be linked to any other entity during its entire lifetime.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Key

All certificate signing requests shall be signed using the private key of the key pair pertaining to the certification request. The certificate signing request format shall be PKCS#10. This signing shall be sufficient proof of possession of the private key.

3.2.2 Authentication of Organization Identity

PK-GRID-CA verifies the Authentication of Organization by checking that:

- The organization is known to be part of a grid-computing project or is a working partner in HEP experiments on recommendation of Regional Centre Manager at NCP.
- The organization is registered and operates in Pakistan. Registration in Pakistan will be validated through proper public authorities.

3.2.3 Authentication of Individual Identity

3.2.3.1 Person Requesting a Certificate

- The subject must contact personally the CA/RA staff in order to verify his identity and the validity of the request.
- The subject authentication is performed through the presentation of a valid official identification document: passport; identity card, and photocopies of these documents are kept in CA record.

3.2.3.2 Host certificate

The request for host certificate should be made through online secure CA portal using personal PK-GRID-CA certificate. Furthermore, the request must be endorsed by the concerned RA through the same portal.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

See section 3.2.2 & 3.2.3.

3.2.6 Criteria of Interoperation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and authentication for Routine re-key

Expiration warnings are sent to subscribers 20, 10 and 5 days ahead of re-key due time. The CA will allow routine re-keying before expiration of the subscriber's current certificate. The re-key request must be accompanied by a request based on a new key pair generated with the help of PK-GRID-CA secure online portal using his existing valid certificate. Certificates must only be re-keyed consecutively for a period of 5 years. After that, the user must follow the same authentication procedure as for a new certificate.

3.3.2 Identification and authentication for re-key after revocation

Applicants without a valid certificate from the PK-GRID-CA (in case of revocation or expiration of certificate) shall be re-authenticated by the CA/RA on certificate application, just as with a first time application.

The applicant should present identification documents mentioned in 3.2.3.1 for rekey requests after expiration or revocation of his certificate. The DN issued to one user is not issued to any other individual even after he drops out of the rekey chain.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Certificate revocation requests should be submitted:

- Through the online secure CA portal using personal PK-GRID-CA certificate.
- When online portal is not an option, the request will be authenticated using the procedure described in section 3.2.3.

4. Certificate Life-cycle Operational Requirements

4.1 CERTIFICATE APPLICATION

4.1.1 Who can submit a Certificate Application

The necessary provisions that must be followed in any certificate application request to the PK-GRID-CA are:

- The subject must be an acceptable end user entity, as defined by this policy.
- The request must obey the PK-GRID-CA distinguished name scheme.
- The distinguished name must be unambiguous and unique.
- The key must have at least 2048 bits.
- The applicants must generate their own key pair.
- The PK-GRID-CA must not know or generate private key for an applicant.
- Host Certificate requests may also be submitted via signed e-mail to pkgrid-ca@ncp.edu.pk
- The default validity period of the certificate is 400 days.

4.1.2 Enrollment Process and Responsibilities

For user certificates, the subject requests an appointment with the CA/RA (in person). The authentication according to sections 1.3.3, 3.2.2 and 3.2.3 must be processed in a face to face meeting. After a successful authentication, the CA/RA process and sign the request.

For host certificates, the person managing the host must send the certificate request via secure online CA portal using a valid PK-GRID-CA personal certificate. The authentication is performed according to sections 1.3.3, 3.2.2 and 3.2.3.

Subscribers Obligations:

Subscribers must be complying with the following:

- Select a strong passphrase for the private key containing minimum 12 characters
- Notifying immediately the PK-GRID-CA and any relying parties if the private key is lost or compromised;
- Requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:
- Use the certificate for the permitted purposes only
- Read and adhere to the procedures published in this document

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

The certificate applications will be validated by the CA/RA. For new user/host certificate request the CA/RA will authenticate the request according to sections 3.2.2 and 3.2.3. The subscriber will request through secure online portal, and the request would subsequently

be endorsed by the concerned RA using the same portal. Occasionally the CA staff may contact the RA over phone for confirmation of the request/endorsement.

4.2.2 Approval or Rejection of Certificate Applications

The PK-GRID-CA will reject certificate applications that are not legitimate. It will inform the requestor via e-mail. Meaningless requests will be discarded without any notification. Also the requests having incomplete documentation may also be discarded after 30 days time-period. The key pairs must be generated by their associated applicants themselves. PK-GRID-CA will never itself generate a key pair on behalf of any applicant.

The necessary provisions that must be followed in any certificate application request to the PK-GRID-CA are:

- The certificate application must be authenticated by the RA as described in section 4.2.1.
- The subject must be an acceptable subscriber entity as defined in section 1.3.3.
- The request must obey the PK-GRID-CA distinguished name scheme.
- The distinguished name scheme must be unambiguous and unique.
- The private key of the end entity must be at least 2048 bits long.

If at least one of the above criteria is not fulfilled by the applicant, the request will be rejected and a signed notification e-mail will be sent to the applicant.

4.2.3 Time to Process Certificate Applications

After the verification of the certificate request has been completed, the certificate is issued. In normal case, this will not take more than five (05) working days.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Upon receiving a certificate request, the CA/RA will verify the compliance and validity of any documents presented by the subscribers. In case of the successful authentication only, the certificate request will be transferred to the signing machine which is not connected to any network. Here the certificate is signed. The PK-GRID-CA will issue the signed certificate which will then be informed to the subscriber at the e-mail address specified in the request.

On the subscriber's request, alternative communication means may be selected. In case of communication failure on permanent basis, the certificate may be revoked without any further notice. The subscriber will also be informed in case of unsuccessful authentication via email also stating the reason.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Right after the issuance of the certificate the CA will send a signed e-mail to the subscriber with information on how to download the certificate from the PK-GRID-CA online server.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers of PK-GRID-CA are required to agree with the following issues:

- Key pair (public key and private key) generation at the end of EE using PK-GRID-CA's secure web portal
- Enrollment procedure as described under section 4.1.2 of this CP/CPS
- Provision of correct information to the PK-GRID-CA regarding the corresponding EE certificate
- Use of the certificate for only authorized purposes that are stated in this document
- Acceptance of conditions and sincerity to the procedures interpreted in this document.

4.4.2 Publication of the Certificate by the CA

PK-GRID-CA users are notified via signed emails about their signed certificates. PK-GRID-CA will publish all valid certificates in an online repository available at the URL: <https://www.ncp.edu.pk/pk-grid-ca/validcerts.php>

4.4.3 Notification of Certificate Issuance by the CA to other Entities

PK-GRID-CA does not notify any other entities about a certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

PK-GRID-CA has no access, nor does it generate the key pair for the subscribers. The certificates issued by the PK-GRID-CA shall be used according to sections 1.4.1 and 3.1.5. The certificates shall not be used for purposes described in section 1.4.2.

4.5.2 Relying Party Public Key and Certificate Usage

Subscribers' public keys and certificates can be used by the Relying Parties for:

- Email signature validation and decryption, server authentication and communication encryption, users/hosts/services authentication in research and grid infrastructures.
- The relying party must consult the current CRL and implement its restrictions while validating certificates.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances for Certificate Renewal

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.2 Who May Request Renewal

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.3 Processing Certificate Renewal Requests

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.4 Notification of New Certificate Issuance to Subscriber

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.6 Publication of the Renewal Certificate by the CA

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

PK-GRID-CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

Subscribers must regenerate their key pair in the following circumstances:

- Expiration of their PK-GRID-CA signed certificate.
- Revocation of their certificate by the PK-GRID-CA.
- If the current private key is suspected to be compromised.

4.7.2 Who May Request Certification of a New Public Key

See section 4.1.1

4.7.3 Processing Certificate Re-keying Requests

Re-key request before expiration of the user certificate can be accomplished by sending a request through secure online CA portal. Re-key request in case of revocation or compromise of the current certificate follows the same procedure as for a new certificate. The certificates are re-keyed for the same subscriber for five years using same set of authentication documents (which were used to authenticate him for the first time); however rekey requests after five years follow the same procedure as for a new certificate.

4.7.4 Notification of new Certificate Issuance to Subscriber

See section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

PK-GRID-CA will publish all valid certificates in an online repository available at the URL: <https://www.ncp.edu.pk/pk-grid-ca/validcerts.php>

4.7.7 Notification of Certificate Issuance by the CA to other Entities

See section 4.4.3

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.2 Who May Request Certificate Modification

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.3 Processing Certificate Modification Requests

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.4 Notification of New Certificate Issuance to Subscriber

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.6 Publication of the Modified Certificate by the CA

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

PK-GRID-CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

A certificate will be revoked in the following circumstances:

- The subject of the certificate has ceased his relation with the PK-GRID projects.
- The subject does not require the certificate any more.
- The private key has been lost or is suspected to be compromised.
- The information in the certificate is wrong or inaccurate.
- The system to which the certificate has been issued has been retired.
- The subject has failed to comply with the rules of this policy.

In case the information in the certificate is not valid or the private key is compromised, the subscriber must inform the CA and request revocation within one working day of the changes and/or the suspected compromise.

4.9.2 Who Can Request Revocation

The revocation of the certificate can be requested by:

- The certificate subscriber in case of user certificate
- The appropriate RA
- The CA
- Any other entity presenting proof of knowledge that the private key has been compromised or that the subscriber's data has been modified

4.9.3 Procedure for Revocation Request

The entity requesting the revocation must send the revocation request through secure online CA portal within one (01) working day of the compromise proof. If this is not possible the CA/RA must be contacted directly. Authentication will be performed as described in 3.2.3.

4.9.4 Revocation Request Grace Period

Revocation request grace-period is one (01) working day.

4.9.5 Time within which CA must Process the Revocation Request

The CA time for processing revocation request is within one (01) working day normally.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties must download the CRL from the online repository at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL Issuance Frequency

CRLs are issued after every certificate revocation or at most every twenty-three (23) days. i.e., 7 days before the expiration of the maximum lifetime for a CRL i.e. 30 days. The CRL is published (in DER format) immediately after its issuance.

4.9.8 Maximum Latency for CRLs

The maximum latency for CRLs is immediately after revocation.

4.9.9 On-line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Re-key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

PK-GRID-CA does not suspend certificates.

4.9.14 Who can Request Suspension

PK-GRID-CA does not suspend certificates.

4.9.15 Procedure for Suspension Request

PK-GRID-CA does not suspend certificates.

4.9.16 Limits on Suspension Period

PK-GRID-CA does not suspend certificates.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The PK-GRID-CA operates as an online repository that contains all the CRLs that have been issued. Promptly following revocation the CRL in the repository shall be updated.

4.10.2 Service Availability

The PK-GRID-CA online repository is maintained on a best effort basis with an intended availability of 24x7. All foreseen/scheduled downtimes in the repository shall be announced to PMA and as widely as possible.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

The subscription ends with the expiry of the certificate if it is not rekeyed before that date, or if the subscriber requests the revocation of the certificate.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

PK-GRID-CA will not accept any key escrow or recovery services and will not give keys on escrow as well.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management and Operational Controls

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The PK-GRID-CA is located in National Centre for Physics at Quaid-i-Azam University Campus, Shahdra Valley Road, Islamabad, Pakistan. Its postal address is as under:

National Centre for Physics
Quaid-i-Azam University Campus
Shahdra Valley Road
Islamabad - 44000
Pakistan
Phone: (+92 – 51) 207 7300
Fax: (+92 – 51) 207 7393
E-mail: pkgrid-ca@ncp.edu.pk

5.1.2 Physical Access

The access to the PK-GRID-CA is restricted to the authorized personnel only. The signing machine is kept behind a locked premises, being accessed only when in use. The physical access mechanism is described in Appendix – A.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the repository machines are connected to a UPS system.

5.1.4 Water Exposures

The CA premises have no history of floods but as a precaution all CA setup and backup is placed on the first floor above ground level.

5.1.5 Fire Prevention and Protection

PK-GRID-CA premises do have fire/smoke alarm system which will help to protect against any consequent mishap.

5.1.6 Media Storage

The PK-GRID-CA key and Back-up copies of PK-GRID-CA related information is kept in several removable storage media.

5.1.7 Waste Disposal

Waste carrying potential confidential information, such as old floppy disks, are physically destroyed before being trashed.

5.1.8 Off-site backup

No off-site backup is currently being taken. Important configuration files, user record and CA private key is backed up in a different building in the same site.

5.2 PROCEDURAL CONTROLS

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.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The CA setup requires persons familiar with PKI concepts. The persons are allocated by the CA manager in NCP.

5.3.2 Background Check Procedures

PK-GRID-CA personnel are recruited from the National Centre for Physics. Hence, the background check procedures for recruitment in NCP are already in place.

5.3.3 Training Requirements

Internal training is provided in case of new inductions by explaining certificate's life cycle and in terms of guidelines mentioned in CA operation manual.

5.3.4 Retraining Frequency and Requirements

Periodic check is performed on the operations performed by CA operators. If found any incompliance with the CPS/operation manual, appropriate trainings are provided.

5.3.5 Job Rotation Frequency and Sequence

No job rotation is being performed here.

5.3.6 Sanctions for Unauthorized Actions

If an unauthorized action is observed, the CA manager may revoke the privileges concerned.

5.3.7 Independent Contractor Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

For carrying out CA operations, the concerned personnel are given a copy of CP-CPS, and a document describing how to implement the procedures.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

- Boots and shutdowns of the equipment
- Interactive system logins

5.4.2 Frequency of Processing Log

Audit logs will be analyzed once per month.

5.4.3 Retention Period for Audit Log

Audit logs will be retained for at least three (03) years.

5.4.4 Protection of Audit Log

Only authorized PK-GRID-CA personnel is allowed to view and process audit logs. Audit logs are copied to an offline medium.

5.4.5 Audit Log Backup Procedures

Audit logs are copied to an offline medium, which is safely stored.

5.4.6 Audit Collection System (internal vs. external)

The audit collection system is internal to the PK-GRID-CA.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

The following data and files will be archived by the PK-GRID-CA:

- All certificate requests including certification and revocation. (in soft form)
- All issued certificates and all issued CRLs. (in soft form)
- All the e-mail messages sent and received by the PK-GRID-CA. (both in soft and hard form)
- All interactive events pertaining to the CA server machine are recorded. (in hard form)

5.5.2 Retention Period for Archive

Logs will be kept for a minimum of three (03) years.

5.5.3 Protection of Archive

All soft form records are backed up on removable media, which are safely stored.

5.5.4 Archive Backup Procedures

Records are archived as soon as a certificate/CRL is issued or at least after every 30 days.

5.5.5 Requirements for Time-stamping of Records

No stipulation.

5.5.6 Archive Collection System (internal or external)

The archive collection system is internal to the PK-GRID-CA.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 KEY CHANGEOVER

PK-GRID-CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new PK-GRID-CA private key should be generated one year before the expiration of the old key. From that point on new certificates are signed by the newly generated signing key. The new PK-GRID-CA public key is posted in the on-line repository. The older but still valid certificate must be available to verify old signatures and its private key must be used to sign CRLs until all the certificates signed using the associated key have expired or been revoked.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If the PK-GRID-CA private key is compromised or destroyed, the CA will:

- Generate a new key pair
- Terminate the issuance and distribution of certificates and CRLs and any other associated services
- Notify subscribers, peer CAs, RAs, and Relying Parties
- Notify relevant security contacts

As far as an End Entity Certificate's private key compromise is concerned the course of action will be according to section 4.9.

5.7.2 Computing Resources, Software, and/or Data are corrupted

In case of any such corruption, the data is recovered from the backup copy.

5.7.3 Entity Private Key Compromise Procedures

See section 5.7.1.

5.7.4 Business Continuity Capabilities after a Disaster

Disaster recovery procedure is documented in Appendix – B.

5.8 CA or RA TERMINATION

Upon termination the PK-GRID-CA will:

- Terminate the issuance and distribution of certificates and CRLs.
- Inform EUGridPMA
- Notify subscribers and Relying Parties.
- Notify relevant security contacts.
- Notify as widely as possible regarding the end of the service.
- Revoke all certificates
- Generate and publish CRL
- Destroy all copies of private keys

6. Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Each subscriber must generate his/her own key pair. The PK-GRID-CA does not generate private keys for subjects. The private key should not be known by other than the authorized user of the key pair. The subscriber/end-entity must also ensure to use a strong passphrase for protection of the private key.

6.1.2 Private Key Delivery to Subscriber

Each subscriber must generate his/her own key pair. PK-GRID-CA does not generate private keys to subscribers, hence, does not deliver private keys to subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

An electronic Certificate Signing Request (CSR) must be submitted with the public key by the entity. The request is made via a secure online CA portal.

6.1.4 CA Public Key Delivery to Relying Parties

PK-GRID-CA public key can be downloaded from the PK-GRID-CA web site at:
<https://www.ncp.edu.pk/pk-grid-ca>

6.1.5 Key sizes

- The key length for a personnel or server certificate is at least 2048 bit.
- The PK-GRID-CA key length is 4096 bits.

The algorithm used for key generation by the PK-GRID-CA is SHA-256.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Key usage is only warranted for authentication and signing proxy certificates. Other key usage bits may be set, but are not warranted under this and any old policy. Certificates and CRLs are signed using the PK-GRID-CA private key. Subscriber keys may also be used for

authentication, message integrity and session key establishment. The keyUsage bits in the certificates are set for instance to support these purposes, but for legacy compatibility, the data encryption and non-repudiation bits may be flagged in specific subscriber certificates.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

6.2.2 Private Key (n out of m) Multi-person Control

No stipulation.

6.2.3 Private Key Escrow

PK-GRID-CA keys are not given in escrow.

6.2.4 Private Key Backup

The PK-GRID-CA private key is kept encrypted in multiple copies in several removable storage media in safe places. The passphrase for the private key is in a sealed envelope kept in a safe place.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

The CA private key is activated by a passphrase which must be at least 15 characters long. The subscriber should also put reasonable effort in protecting the private key and the associated passphrase. The subscriber must use a passphrase of at least 12 characters long following best practices for high-quality passwords.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The PK-GRID-CA archives its public key in an online repository and an offline backup copy is also kept.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The PK-GRID-CA private key has currently a validity of ten (10) years.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The PK-GRID-CA private key is protected by a passphrase with a minimum length of 15 characters.

6.4.2 Activation Data Protection

PK-GRID-CA uses a passphrase to activate its private key which is known only by the PK-GRID-CA personnel. A copy in written form of the passphrase is kept in a sealed envelope in a safe. Access to the safe is restricted only to the PK-GRID-CA personnel.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

- The operating systems of CA computers are maintained at a high level of security by applying all the relevant patches.
- CA's system configuration is reduced to the bare minimum.
- The signing machine is kept powered off between uses.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

- The CA signing machine is kept off-line not connected to any kind of network.
- The machines containing CA repository other than the signing machine are protected by a hardware firewall and an Intrusion Detection and Prevention System (IDP).

6.8 TIME-STAMPING

No stipulation.

7. Certificate, CRL and OCSP Profiles

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

All certificates that reference this Policy will be issued in the X.509 version 3 format and will include a reference to the O.I.D. of this Policy within the appropriate field.

7.1.2 Certificate Extensions

PK-GRID-CA supports following certificate profile:

For user certificates:

- Basic Constraints: critical, ca: false
- Subject Key Identifier: hash
- Key Usage: critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation
- Extended Key Usage: clientAuth, emailProtection, Microsoft Encrypted File System
- CRL Distribution Points: URI
- Certificate Policies: OID of this CP (see 7.1.6) and OID of the Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure (which is: 1.2.840.113612.5.2.2.1)
- Subject alternative name: RFC822 Name (email address of subscriber)
- Issuer alternative name: email address of PK-GRID-CA

For servers/services certificates:

- Basic Constraints: critical, ca: false
- Subject Key Identifier: hash
- Key Usage: critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation
- Extended Key Usage clientAuth, serverAuth, emailProtection, Microsoft Encrypted File System
- CRL Distribution Points: URI
- Certificate Policies: OID of this CP (see 7.1.6) and OID of the Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure (which is: 1.2.840.113612.5.2.2.1)
- Subject alternative name: Server's DNS FQDN host name
- Issuer alternative name: email address of PK-GRID-CA

For CA certificate:

- Basic Constraints: critical, ca: true
- Key Usage: critical, KeyCertSign, cRLSign
- CRL Distribution Points: URI
- Subject alternative name: email address of PK-GRID-CA

- Subject key identifier: Subject key identifier will be valid from Dec 2016 onwards when the new Root Cert will be issued
- Authority key identifier: Authority key identifier will be valid from Dec 2016 onwards when the new Root Cert will be issued

7.1.3 Algorithm Object Identifiers

The OIDs for algorithms used for signatures for certificates issued by the PK-GRID-CA are according to:

- Hash Function: id-sha256 2.16.840.1.101.3.4.2.1
- RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
- Signature Algorithm: sha256WithRSAEncryption 1.2.840.113549.1.1.11

7.1.4 Name Forms

Issuer:

C=PK,
O=NCP,
CN=PK-GRID-CA

Subject (Persons):

C=PK,
O=NCP,
OU=<ORG UNIT>,
CN=<FULL NAME>

Subject (Hosts):

C=PK,
O=NCP,
OU=<ORG UNIT>,
CN=<FQDN>

7.1.5 Name Constraints

As described in sections 3.1.1 and 3.1.2.

7.1.6 Certificate Policy Object Identifier

- PK-GRID-CA identifies this policy with the object identifier (O.I.D.): 1.3.6.1.4.1.19323.1.1.3.3

This OID is constructed as follows:

IANA	1.3.6.1.4.1
NCP	.19323
ASC	.1
CP-CPS	.1
Major Version	.3
Minor Version	.3

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version Number(s)

PK-GRID-CA creates and publishes X.509 version 2 DER format CRLs signed with Sha1RSA algorithm (soon to be switched to sha2). All the CRLs will be RFC 5280 compliant except that the Subject key identifier and authority key identifier will be valid from Dec 2016 onwards when the new Root Certificate will be signed.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. Compliance, Audit and other Assessments

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Compliance assessment is performed once a year by an internal audit activity. Requests for external audit from other trusted CAs may be considered at the discretion of National Centre for Physics with the consideration that all costs associated with such an audit will be borne by the requesting party.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

No stipulation.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

No stipulation.

8.4 TOPICS COVERED BY ASSESSMENT

The assessment would cover all the topics that would ensure that the policies and procedures being followed being practiced by the CA are in compliance with the approved CP-CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The CA will announce the steps that will be taken to fulfill the deficiency within a suitable time-period. If a deficiency revealed has direct impacts on the security and the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

8.6 COMMUNICATION OF RESULTS

The CA Manager will publish the results with as much detail as he deems fit.

9. Other Business and Legal Matters

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No fees shall be charged.

9.1.2 Certificate Access Fees

No fees shall be charged.

9.1.3 Revocation or Status Information Access Fees

No fees shall be charged.

9.1.4 Fees for Other Services

No fees shall be charged.

9.1.5 Refund Policy

No fees shall be charged therefore there is no refund policy.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No financial responsibility is accepted for any certificate issued under this or any old policy.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

No Stipulation.

9.3.2 Information not within the Scope of Confidential Information

No Stipulation.

9.3.3 Responsibility to Protect Confidential Information

No Stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

Record of the e-mail messages sent and received by the PK-GRID-CA and the information in the ID documents for identity validation is considered confidential. Under no circumstances, does the PK-GRID-CA have access to the private keys of the subscribers to whom it issues a certificate.

9.4.1 Privacy Plan

See section 9.4

9.4.2 Information Treated as Private

See section 9.4

9.4.3 Information not Deemed Private

The PK-GRID-CA collects the following information from the subscriber:

- Subscriber's full name
- Subscriber's e-mail address
- Subscriber's organization
- Subscriber's organizational unit
- Subscriber's public key

which is not considered confidential.

9.4.4 Responsibility to Protect Private Information

See section 9.4

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The PK-GRID-CA will not disclose any information to any third party, aside from information publicly available, except when so required by a legal authority of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

See section 9.4.6

9.5 INTELLECTUAL PROPERTY RIGHTS

This CP-CPS is structured according to RFC 3647, and is inspired by:

- RFC 2527 and RFC 3647
- DutchGrid and NIKHEF Medium-Security X.509 CA CP/CPS v3.0
- EG-Grid CA CP/CPS
- Authentication Profile for Classic X.509 Public Key CAs with Secured Infrastructure Version 4.4

PK-GRID-CA does claim no intellectual property rights on issued certificates, practice/policy specifications, names or keys. In addition, it allows redistribution of this CP/CPS by EU-Grid-PMA or any of its accredited federations without explicit permission.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

No stipulation.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

PK-GRID-CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness. Also PK-GRID-CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

9.8 LIMITATIONS OF LIABILITY

PK-GRID-CA:

- Guarantees only to authenticate the subjects requesting a certificate or revocation request according to the procedures described in this document; no other liability, neither implicit nor explicit is accepted.
- Is run on a best effort basis and does not give any guarantees about the service security or suitability.
- Will not be held liable for any problems arising from its operation or use made of certificates it issues.
- Denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

9.9 INDEMNITIES

PK-GRID-CA declines any payment of indemnities for damages arising from the use or rejection of its issued certificates.

9.10 TERM AND TERMINATION

9.10.1 Term

This document becomes effective after its accreditation by the PMA and publication on the PK-GRID-CA website.

9.10.2 Termination

This document remains effective until it is superseded by a newer version or until any further notice.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

No stipulation.

9.12.2 Notification Mechanism and Period

PK-GRID-CA doesn't explicitly inform subscribers about any updates in its CP/CPS. The update is made locally first, gets approval from its local management and then by EU-Grid-PMA, only after which it gets published on the web. The certificates issued onwards are influenced under the approved modifications.

9.12.3 Circumstances under which OID must be changed

Whenever any major or minor change is made in the document either in its structure or contents, the existing OID would be modified accordingly.

9.13 DISPUTE RESOLUTION PROVISIONS

Disputes arising out of the CP/CPS shall be resolved by the PK-GRID-CA manager(s).

9.14 GOVERNING LAW

The enforceability, construction, interpretation, and validity of this policy shall be governed by the Laws of Pakistan.

9.15 COMPLIANCE WITH APPLICABLE LAW

All activities relating to the certification request, issuance, use or acceptance of the PK-GRID-CA certificates must comply with the Pakistan's Law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

APPENDIX – A

PHYSICAL ACCESS TO PK-GRID-CA

Physical access to the PK-GRID-CA is restricted to authorized personnel only. PK-GRID-CA system are protected by a minimum of three zones of physical security namely Blue, Yellow and Red Zone, with access to the lower zone required before gaining access to the higher zone. Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur with very restrictive physical tiers. Following are the key-points regarding each security zone.

- Access to the Blue Zone entails authentication mechanism via an RFID card (employee badge).
- Access to the Yellow Zone involves employee PIN authentication in addition to the RFID card system (two factor authentication).
- The Red zone's access procedure requires a triple level verification mechanism including RFID card, entering PIN as well as biometric authentication i.e. Thumb impression recognition system.
- Physical access is automatically logged (card reader devices) and video recorded for each of the three zones.
- The Red Zone can only be accessed in the presence of two persons (CA Managers).
- Unescorted personnel, including un-trusted employees (other than CA staff) or visitors, are not allowed in yellow and red zones.
- The opening and closing of cabinets or containers in these tiers are logged for audit purposes.

The Blue Zone is the main operation centre for general PK-GRID-CA operations, and includes facilities like customer's desk, information/help desk.

The Yellow Zone is more restrictive in nature. It may contain offices of CA personnel. Access is controlled by locked doors. (Card reader + PIN verification devices).

The Red Zone is the most restrictive zone among the three. All the vital CA operations e.g. key signing; CRL signing etc. will take place there. It can be opened only in the presence of two CA managers. The door on the red zone has a dual person authentication facility (RFID cards and pin codes, plus the thumb scans for both personnel is required to open it). Every movement in red zone is captured via video recording, and opening and closing of cabinets are also recorded. This zone should also contain a safe where the secret keys can be stored safely. All activities with the CA signing machine e.g. boots and shutdowns are recorded as well.

APPENDIX – B**BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER**

To cope up with natural and manmade disasters, a replica comprising of all the essential items needed to run the CA setup has been created. Due to lack of access to any other suitable premises for the time being, the backup material is residing in the same premises but of course under a separate building. Although the premises and surrounding area has no history of floods, as a precaution all CA setup and backup are kept on first floor above ground level. All the corresponding stuff is being placed inside a secure safe access to which is limited to the concerned personnel (CA managers and CA operations staff) only. Following items constitute the replica:

- CA root private (with passphrase) and public keys.
- Copy of user record such as their necessary documents and email correspondence.
- Necessary setup and configuration files.