PK-GRID-CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Document OID: 1.3.6.1.4.1.19323.1.1.2.0

Prepared By:

National Centre for Physics (NCP),
Quaid-i-Azam University Campus, Islamabad
Ph: (+ 92 - 51) 260 1018, Fax: (+92 - 51) 920 5753
URL: http://www.ncp.edu.pk

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.: **1.3.6.1.4.1.19323.1.1.2.0**
- Document Date: **December 2007.**
- 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. Currently, following Registration Authorities (RAs) are recognized by PK-Grid-CA:

- NCP
- PAEC

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 of GRID computing infrastructure, that are using the public keys in 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
Advanced Scientific Computing
National Centre for Physics
Quaid-i-Azam University Campus
Islamabad - 45320
Pakistan
Phone: (+92 - 51) 260 1018
Fax: (+ 92 - 51) 920 5753
Email: pkgrid-ca@ncp.edu.pk

1.5.2 Contact Person

The contact person for questions related with this document and PK-Grid-CA operation is:

Usman Ahmad Malik
Advanced Scientific Computing

National Centre for Physics
Quaid-i-Azam University Campus
Islamabad - 45320
Pakistan
Phone: (+92 - 51) 260 1018
Fax: (+ 92 - 51) 920 5753
Email: usman.malik@ncp.edu.pk

1.5.3 Person Determining CPS Suitability for the Policy

The person determining the CPS suitability if the policy is:

Sajjad Asghar
Advanced Scientific Computing
National Centre for Physics
Quaid-i-Azam University Campus
Islamabad - 45320
Pakistan
Phone: (+92 - 51) 260 1018
Fax: (+ 92 - 51) 920 5753
Email: sajjad.asghar@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.

SHA1

SHA stands for **S**ecure **H**ash **A**lgorithm. 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.

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 repositories are published at the URL http://www.ncp.edu.pk/pk-grid-ca
The address for issues regarding the repositories is:

PK-GRID Certification Authority
National Centre for Physics
Quaid-i-Azam University Campus
Islamabad - 45320
Pakistan
Phone: (+92 – 51) 260 1018
Fax: (+92 – 51) 920 5753
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 this document, which specifies the CP and CPS.
- Other relevant information.

The online repositories are published at the following URL:
http://www.ncp.edu.pk/pk-grid-ca

All valid certificates are published at the following URL:
http://www.ncp.du.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.

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". The subscribers class, defined as "people" or "host" shall be attached in the form "O=Class". The "people" class will contain certificates for subscribers that are natural persons. The "host" class will contain certificates for subscribing entities that are automated systems or applications.

- For a user certificate the common name (CN) name must be the full name of the subscriber.

- In case the subscriber belongs to the "host class" the subject 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.

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

No stipulation.

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.

3.2.3.2 Host certificate

Requests must be signed with the personal PK-Grid-CA certificate of the corresponding system administrator who is responsible for that machine or host name.

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

For re-key the subject will submit the request through PK-Grid-CA online portal along with a signed email with valid personal PK-Grid-CA 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.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Certificate revocation requests should be submitted by:

- E-mail sent to pkgrid-ca@ncp.edu.pk signed with a valid PK-Grid-CA certificate followed by procedure defined in 3.2.3.
- When e-mail 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 1024 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 one (01) year.

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 signed e-mail (signed with a valid PK-Grid-CA personal certificate), along with the certificate request through online portal. The authentication is performed according to sections 1.3.3, 3.2.2 and 3.2.3.

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 certificate request the CA/RA will authenticate the request according to sections 3.2.2 and 3.2.3.

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 1024 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

No stipulation.

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: http://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 section 1.4.1. 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 an email signed with the current user certificate. Re-key request after expiration follows the same authentication procedure as for a new certificate. Re-key request in case of

revocation or compromise of the current certificate follows 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: http://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.

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 by signed e-mail to the PK-Grid-CA/RA. 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 least every twenty-three (23) days. i.e., 7 days before the expiration on the maximum lifetime for a CRL i.e. 30 days.

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.

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, Islamabad, Pakistan.

National Centre for Physics
Quaid-i-Azam University Campus
Islamabad - 45320
Pakistan
Phone: **(+92 – 51) 260 1018**
Fax: **(+92 – 51) 920 5753**
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 locked in a safe, being accessed only when in use.

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

No stipulation.

5.1.5 Fire Prevention and Protection

No stipulation.

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.

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

No stipulation.

5.3.4 Retraining Frequency and Requirements

No stipulation.

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).
- All issued certificates and all issued CRLs.
- All the e-mail messages sent and received by the PK-Grid-CA.

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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.

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

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

No stipulation.

5.8 CA or RA TERMINATION

Upon termination the PK-Grid-CA will:

- Terminate the issuance and distribution of certificates and CRLs.
- Notify subscribers and Relying Parties.
- Notify relevant security contacts.
- Notify as widely as possible the end of the service.

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.

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/non-secure public website.

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:
http://www.ncp.edu.pk/pk-grid-ca

6.1.5 Key sizes

1. The key length for a personnel or server certificate is 1024 bit.

2. The PK-Grid-CA key length is 4096 bits

The algorithm used for key generation by the PK-Grid-CA is SHA1.

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 private key is activated by a passphrase.

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

- Basic constraints (Critical):

  Not a CA.

- Subject key identifier
- Subject alternative name
- Issuer alternative name
- CRL distribution points
- Certificate policies

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer:
C=PK,
O=NCP,
CN=PK-Grid-CA

Subject (Persons):
C=PK,
O=NCP,
O=People,
OU=<ORG UNIT>,
CN=<FULL NAME>
EMAIL=<EMAIL ADDRESS>

Subject (Hosts):
C=PK,
O=NCP,
O=Host,
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.): **1.3.6.1.4.1.19323.1.1.2.0.** This OID is constructed as follows:

IANA	1.3.6.1.4.1
NCP	.19323
ASC	.1
CP-CPS	.1
Major Version	.2
Minor Version	.0

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)

All CRLs will be CRL version 2 format.

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.

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
- RomanianGrid CA CP/CPS
- Authentication Profile for Classic X.509 Public Key CAs with Secured Infrastructure

PK-Grid-CA does claims no intellectual property rights on issued certificates, practice/policy specifications, names or keys

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

No stipulation.

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

No stipulation.

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

No stipulation.

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.