PK-GRID-CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Document OID: 1.3.6.1.4.1.19323.1.1.1.4

Prepared By:

National Centre for Physics (NCP),
Quaid-I-Azam University Campus, Islamabad
Ph: (92-51) 2273545, Fax: (92-51) 9205753
URL: http://www.ncp.edu.pk

Table of Contents

1. Introduction

1.1 OVERVIEW

This document is based on the structure suggested by the RFC 2527. It defines the Certification 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. Terms used in this document are explained in the Glossary.

1.2 POLICY IDENTIFICATION

- Document Title: **'PK-Grid-CA Certificate Policy and Certification Practice Statement'**
- Document O.I.D.: **1.3.6.1.4.1.19323.1.1.1.4**
- Document Date: **April 2004.**
- Expiration: This document is valid until further notice.

1.3 COMMUNITY AND APPLICABILITY

PK-Grid-CA provides PKI services for scientific communities of Pakistan, which are NCP working partners in Grid related projects.

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 are recognized by PK-Grid-CA:

- COMSATS
- NUST
- 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 End Entities

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 Applicability

There are two categories of certificates:

1. User certificates: authentication and communication encryption.

2. Host certificates: authentication and communication encryption.

1.3.5 User Restrictions

Certificates issued by the PK-Grid-CA are only valid in the context of the Grid activities in Pakistan. Any other usage such as financial transactions is strictly forbidden. The ownership of a PK-Grid certificate does not imply automatic access to any kind of resources.

1.4 CONTACT DETAILS

The PK-Grid-CA is created and managed by the Advanced Scientific Computing Group, National Centre for Physics.

The PK-Grid-CA address for operational issues is:

PK-Grid Certification Authority
Advanced Scientific Computing
National Centre for Physics
Quaid-I-Azam University
Islamabad - 45320
Pakistan
Phone: (+92 - 51) 2273545
Fax: (+ 92 -51) 9205753
Email: pkgrid-ca@ncp.edu.pk

The contact person for questions related with document is:

Usman Ahmad Malik
Advanced Scientific Computing
National Centre for Physics
Quaid-I-Azam University
Islamabad - 45320
Pakistan
Phone: (+92 - 51) 2273545
Fax: (+ 92 -51) 9205753
Email: usman@ncp.edu.pk

The contact person for PK-Grid-CA related issues is:

Sajjad Asghar
Advanced Scientific Computing
National Centre for Physics
Quaid-I-Azam University
Islamabad - 45320
Pakistan
Phone: (+92 - 51) 2273545
Fax: (+ 92 -51) 9205753
Email: sajjad@ncp.edu.pk

2. General Provisions

2.1 OBLIGATIONS

2.1.1 PK-Grid-CA Obligations

The PK-Grid-CA is responsible for the following aspects of issuance and management of certificates:

- Issue and publish certificates based on validated requests.
- Accept certification requests validated by the RA.
- Deliver the certificate to end entity.
- Accept revocation requests from RA's or end entities.
- Ensuring that all aspects of the CA services, CA operations and CA infrastructure, related to certificates issued under this policy, are performed in accordance with the requirements, representations and warranties of this document.

2.1.2 PK-Grid RA Obligations

The PK-Grid RA is responsible for the following aspects:

- Authenticate entities requesting a certificate according to the procedures described in this document.
- Determine if the person requesting the certificate has the right to have a PK-Grid-CA certificate.
- Send validated certificate requests to PK-Grid-CA.
- Create and send validated revocation requests to the PK-Grid-CA.
- Follow the policies and procedures described in this document.

The RA communicates with the PK-Grid-CA via telephonic conversation which is followed by the signed e-mail.

2.1.3 Subscriber Obligations

In all cases, the PK-Grid-CA shall require the subscriber to:

- Read and accept the policies and procedures published in this document.
- Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key.
- Use a strong passphrase with a minimum length of 12 characters to protect the private key of personal certificates.
- Use the certificate exclusively for authorized and legal purposes, consistent with this policy.
- Notify the PK-Grid-CA when the certificate is no longer required.
- Notify the PK-Grid-CA when the information in the certificate becomes wrong or inaccurate.

- Instruct the PK-Grid-CA to revoke the certificate promptly upon an actual or suspected loss, disclosure, or other compromise of the subscriber's private key.
- Accepts the statements relating to confidentiality of information in section 2.8.

2.1.4 Repository Obligations

The PK-Grid-CA is responsible for providing a public repository, accessible through the World Wide Web at http://www.ncp.edu.pk/pk-grid-ca

- PK-Grid-CA will publish its public key on the above website.

- PK-Grid-CA will publish on the above website the CRLs as soon as they are issued.

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 per day, 7 days a week basis.

2.1.5 Relying Party Obligations

A Qualified Relying Party is required to:

- Accept the conditions and procedures described in this document.
- Use the certificate exclusively for authorized and legal purposes, consistent with this Policy.
- Verify the certificate revocation information before validating a certificate.

2.2 LIABILITY

2.2.1 PK-Grid-CA 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.

2.2.2 RA Liability

The Registration Authority:

- Authenticates the identity of the subscribers requesting the certificates, according to the practices described in this policy.
- Requests for revocation of a certificate if it is aware that the circumstances for revocation are satisfied.

2.3 FINANCIAL RESPONSIBILITY

PK-Grid-CA will not accept any financial responsibilities.

2.4 INTERPRETATION

2.4.1 Governing Law

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

2.4.2 Dispute Resolution Procedures

Legal disputes arising from the operation of the PK-Grid-CA will be resolved according to the Pakistan Law.

2.5 FEES

No fees are charged.

2.6 PUBLICATION AND REPOSITORIES

2.6.1 Publication of CA Information

The PK-Grid-CA publishes the following information through its online repository at http://www.ncp.edu.pk/pk-grid-ca:

- The PK-Grid-CA root certificate.
- Issued host and user certificates that reference this policy.
- The latest Certificate Revocation List (CRL).
- A copy of this document, which specifies the CP and CPS.
- Other relevant information.

2.6.2 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.

2.6.3 Access Controls

- 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 in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available on a 24 hours per day, 7days a week basis.

2.7 COMPLIANCE AUDIT

PK-Grid-CA declares that their practices fully comply with this CP-CPS. Requests for external audit from other trusted CA 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.

2.7.1 Frequency of Entity Compliance Audit

No Stipulation.

2.7.2 Identity/qualifications of auditor

No Stipulation.

2.7.3 Auditor's relationship to audited party

No Stipulation.

2.7.4 Topics covered by audit

No Stipulation.

2.7.5 Actions taken as a result of deficiency

No Stipulation.

2.7.6 Communication of results

No Stipulation.

2.8 CONFIDENTIALITY POLICY

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.

2.8.1 Confidential Information kept by the PK-Grid-CA

Record of the e-mail messages sent and received by the PK-Grid-CA 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.

2.8.2 Types of Information not considered Confidential

Data contained in the CRLs and the subscriber certificate shall not be considered confidential and will be published in a publicly accessible location.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

The PK-Grid-CA will notify and inform the following entities:

- The subject of the personal certificate.
- The requester of the server certificate.

2.8.4 Release of Information to Law Enforcement Officials

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.

2.8.5 Information that can be revealed as a Part of Civil Discovery

See section 2.8.4

2.8.6 Conditions of Disclosure upon owner's request

See section 2.8.1

2.8.7 Other Circumstances for Disclosure of Confidential Information

See section 2.8.4

2.9 INTELLECTUAL PROPERTY RIGHTS

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

3. Identification and Authentication

3.1 INITIAL REGISTRATION

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 name.
- In case of server certificate the subject name must include the DNS FQDN.

3.1.2 Name Meanings

- 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 server.

3.1.3 Name Uniqueness

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 are appended to the name to ensure uniqueness. Certificates must apply to unique individuals or resources. Users must not share certificates.

3.1.4 Verification of Key Pair

No Stipulation.

3.1.5 Authentication of Organization

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.

3.1.6 Authentication of Individual

3.1.6.1 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.

3.1.6.2 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 ROUTINE REKEY

Rekey of certificates will follow the same authentication procedure as new certificate. A request for rekeying of a certificate must be submitted prior to certificate expiration.

3.3 REKEY AFTER REVOCATION

Revoked or expired certificates shall not be renewed. Applicants without a valid certificate from the PK-Grid-CA shall be re-authenticated by the RA on certificate application, just as with a first time application.

3.4 REVOCATION REQUESTS

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 3.1.6.
- When e-mail is not an option, the request will be authenticated using the procedure described in section 3.1.6.

4. Operational Requirements

4.1 CERTIFICATE APPLICATIONS

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 validation period is one (1) year.

4.2 CERTIFICATE ISSSUANCE

Following are the requirements for a certificate to be issued:

- The subject authentication must be successful.
- The key must have 1024 bits.
- The maximum validity period for a certificate must be 1 year.

The subject will be notified by e-mail about the certificate issuance or rejection. In the case of rejection the e-mail will state the reason.

4.3 CERTIFICATE ACCEPTANCE

Not defined.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances of 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.

4.4.2 Who can Request Revocation

The revocation of the certificate can be requested by:

- The certificate subscriber.
- Any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data.
- The Registration Authorities (RAs).
- The PK-Grid-CA.

4.4.3 Procedure of 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 can be performed as described in 3.1.6.

4.4.3.1 Repository/CRL Update

The CRL or certificate status database in the repository, as applicable, shall be updated immediately after revocation. All revocation requests and the resulting actions taken by the PK-Grid-CA shall be archived.

4.4.4 Certificate Suspension

There is no provision for certificate suspension.

4.4.5 Who can request suspension

No Stipulation.

4.4.6 Procedure for suspension request

No Stipulation.

4.4.7 Limits on Suspension Period

No Stipulation.

4.4.8 CRL Issuance Frequency

CRLs are issued after every certificate revocation or at least every twenty-three (23) days.

4.4.9 CRL Checking Requirements for Relying Parties

Download the CRL at least once a day and implement its restrictions while validating certificates.

4.4.10 On-line Revocation/Status Checking Availability

Not defined.

4.4.11 On-line Revocation Checking Requirements

Not defined.

4.4.12 Other Forms of Revocation Advertisement

Not defined.

4.4.13 Variations of the above in case of private key compromise

Not defined.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 Types of Events Audited

- Boots and shutdowns of the equipment
- Interactive system logins

4.5.2 Processing Frequency of Audit Logs

Audit logs will be analyzed at least once per month.

4.5.3 Retention Period of Audit Logs

Audit logs will be retained for a minimum of three (3) years.

4.5.4 Protection of Logs

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

4.5.5 Backup Procedures

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

4.5.6 Accumulation system

The audit log accumulation system is internal to the PK-Grid-CA.

4.6 RECORDS ARCHIVAL

4.6.1 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.

4.6.2 Retention Period for Archives

Logs will be kept for a minimum of three (3) years.

4.6.3 Protection of Archive

Records are backed up on removable media, which are safely stored.

4.6.4 Archive Backup Procedures

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

4.6.5 Archive Collection System

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

4.7 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.

4.8 COMPROMISE AND DISASTER RECOVERY

If the PK-Grid-CA private key is destroyed, compromised or suspected to be, the PK-Grid-CA will:

- Notify subscribers and other relying parties.
- Terminate the issuance and distribution of certificates and CRLs.
- Notify relevant security contacts.

4.9 CA TERMINATION

Upon termination the PK-Grid-CA will:

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

5. Physical, Procedural and Personnel Security Controls

5.1 PHYSICAL SECURITY – ACCESS CONTROLS

5.1.1 Site Location

The PK-Grid-CA is located at Quaid-I-Azam University Campus, Islamabad, Pakistan.

5.1.2 Physical Access

Physical access to the PK-Grid-CA is restricted to authorized personnel.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the repository machines are connected to an 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 backups are currently performed.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Not defined.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background Checks and Clearance Procedures for CA Personnel

PK-Grid-CA personnel are recruited from the National Centre for Physics.

5.3.2 Background Checks and Security Procedures for other personnel

No other personnel are authorized to access the PK-Grid-CA facilities without the physical presence of PK-Grid-CA personnel.

5.3.3 Training Requirements and Procedures

Not defined.

5.3.4 Training Period and Retraining Procedures

Not defined.

5.3.5 Frequency and Sequence of Job Rotation

No job rotation is performed.

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 Entity

The PK-Grid-CA does not generate private keys hence does not deliver private keys.

6.1.3 Subscriber Public Key Delivery to PK-Grid-CA

Public keys are delivered by encrypted e-mail, SSL over http.

6.1.4 Public Key delivery to Entity

Public keys are delivered by encrypted e-mail by PK-Grid-CA personnel.

6.1.5 CA Public Key delivery to users

PK-Grid-CA certificate can be downloaded from the PK-Grid-CA web site at:
http://www.ncp.edu.pk/pk-grid-ca

6.1.6 Key Sizes

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

2. The PK-Grid-CA key length is 2048 bits

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

6.1.7 Public Key Parameters Generation

Not defined.

6.1.8 Parameter quality testing

Not defined.

6.1.9 Hardware/software key generation

Not defined.

6.1.10 Key Usage Purposes

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

6.2 PRIVATE KEY PROTECTION

6.2.1 Private Key (n out of m) Multi-Person Control

Not defined.

6.2.2 Private Key Escrow

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

6.2.3 Private Key Archival and Backup

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

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

The PK-Grid-CA private key has currently a validity of five (5) years.

6.4 ACTIVATION DATA

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

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Security Technical Requirements

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

6.5.2 Computer Security Rating

Not defined.

6.6 LIFE CYCLE SECURITY CONTROLS

Not defined.

6.7 NETWORK SECURITY CONTROLS

- The CA signing machine is kept off-line.
- CA/RA machines other than the signing machine are protected by a firewall.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Not defined.

7. Certificate and CRL profile

7.1 CERTIFICATE PROFILE

7.1.1 Version

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=ncp.edu.pk

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=<UNIT>,
CN=<FQDN>

7.1.5 Name Constraints

See section 3.1.2

7.1.6 Certificate Policy Identifier

- PK-Grid-CA identifies this policy with the object identifier (O.I.D.): **1.3.6.1.4.1.19323.1.1.1.4.** This OID is constructed as follows:

IANA	1.3.6.1.4.1
NCP	.19323
ASC	.1
CP-CPS	.1
Major Version	.1
Minor Version	.4

7.1.7 Policy Qualifier Syntax and Semantics

Not defined.

7.2 CRL PROFILE

7.2.1 Version

All CRLs will be CRL version 1 format.

8. Policy Administration

8.1 SPECIFICATION CHANGE PROCEDURES

Relevant changes will be made as widely available as possible.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The PK-Grid-CA policy is available at http://www.ncp.edu.pk/pk-grid-ca

8.3 CPS APPROVAL PROCEDURES

No Stipulation.

9. Versions

9.1 CHANGE LOG

Version 1.1.1.0 Drafted December 2003

Version 1.1.1.1 Drafted January 2004

a) Added ASN.1 OID [1.2]
b) Revised 'Relying Party' obligations [2.1.5]
c) Added 'RA Liabilities' [2.1.2]
d) Clarified CRL publication/issuance frequency [2.6.3]
e) Revised 'Audit Compliance' [2.7]
f) Revised 'Confidentiality Policy' [2.8]
g) Revised 'Name Meanings' [3.1.2]
h) Revised 'Name Uniqueness' [3.1.3]
i) Revised 'Verification of Private Key' [3.1.4]
j) Revised 'Host Certificate' [3.1.6.2]
k) Revised 'Rekey' [3.2]
l) Revised 'Certificate Revocation' [4.4.2]
m) Revised 'keychangeover' [4.7]
n) Revised 'Key Usage Purposes' [6.1.10]
o) Revised 'Private Key Protection' [6.2.2]
p) Increased lifetime of CA certificate to 5 years [6.3]

Version 1.1.1.2 Drafted February 2004

a) Revised 'User Restrictions' [1.3.5]
b) Revised 'Routine Rekey' [3.2]
c) Typing mistakes corrected [1.3, 1.3.2, 6.3]

Version 1.1.1.3 Drafted March 2004

a) Document 'OID' Changed
b) Revised 'Community and Applicability' [1.3]
c) Revised 'Registration Authorities' [1.3.2]
d) Revised 'Applicability' [1.3.4]
e) Typing mistakes corrected [1.4]
f) Typing mistakes corrected [2.1.4]
g) Re-phrased 'RA Liability' [2.2.2]
h) Typing mistakes corrected [2.6.2]
i) 'Subscriber's organizational unit' added [2.8]
j) Typing mistakes corrected [2.8.1]
k) Typing mistakes corrected [2.8.4]
l) Typing mistakes corrected [3.1.2]
m) Revised 'Revocation Requests' [3.4]
n) Typing mistakes corrected [4.1]
o) Revised 'Certificate Applications' [4.1]
p) Re-phrased 'Certificate Issuance' [4.2]

q) Typing mistakes corrected [4.4.3]
r) Revised 'Types of Records Archived' [4.6.1]
s) Revised 'Archive Backup Procedures' [4.6.4]
t) Typing mistakes corrected [4.9]
u) Re-phrased 'Key Sizes' [6.1.6]
v) Revised 'Key Usage Purposes' [6.1.10]
w) Revised 'Name Forms' [7.1.4]
x) Revised 'Version' [7.2.1]

Version 1.1.1.4 Drafted March 2004

a) Revised 'Subscriber Obligations'. Passphrase length changed to 12 [2.1.3]
b) Revised 'Compliance Audit' [2.7]
c) Revised 'Routine Rekey' [3.2]
d) Revised 'Other Aspects of Key Pair Management' [6.3]

Glossary

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 for server certification and encryption of communications (SSL/TSL). 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

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

RSA

RSA is named after its creators Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman. It is the most popular public key algorithm currently in use. It is so popular because it provides secrecy, authentication and encryption all in one little package.

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.