



Indian Grid Certification Authority (IGCA)
Certificate Policy/Certification
Practice Statement

Version 1.1

August 5, 2009

Centre for Development of Advanced Computing (C-DAC),
Bangalore

Document History

Document Name	Document Version	Status	Date	By whom	Review	Remarks
CP/CPS for IGCA	1.0	Created	18/07/2008	Natraj, Henry, Santhosh	Dr. Subrata	Initial
CP/CPS for IGCA	1.0	Created	7/10/2008	Natraj, Henry, Santhosh, Asish	Dr. Subrata	Reviewed by APGridPMA
CP/CPS for IGCA	1.1	Modified	5/8/2009	Henry, Santhosh, Asish	Dr. Subrata	Added Classic AP 4.2 profile OID

Table of Contents

1	Introduction.....	9
1.1	Overview	9
1.2	Document Name and Identification	9
1.3	PKI Participants.....	9
1.3.1	Certificate Authorities	9
1.3.2	Registration Authorities	9
1.3.3	Subscribers (End Entities)	10
1.3.4	Relying parties	10
1.3.5	Other participants.....	11
1.4	Certificate Usage.....	11
1.4.1	Appropriate certificate uses	11
1.4.2	Prohibited certificate uses.....	11
1.5	Policy Administration	11
1.5.1	Organization administering the document.....	11
1.5.2	Contact Details.....	11
1.5.3	Person determining CPS suitability for the policy	11
1.5.4	CPS approval procedures.....	11
1.6	Definitions and Acronyms	11
1.6.1	General Definitions.....	11
2	Publications and Repository Responsibilities.....	12
2.1	Repositories	12
2.2	Publication of Certificate information	12
2.3	Time or frequency of publication.....	13
2.4	Access Controls on repositories	13
3	Identification and Authentication.....	13
3.1	Naming.....	13
3.1.1	Types of names.....	13
3.1.2	Need for names to be meaningful	13
3.1.3	Anonymity of subscribers.....	13
3.1.4	Rules for interpreting various name forms.....	13
3.1.5	Uniqueness of Names	13
3.1.6	Recognition, authentication and role of trademarks.....	14
3.2	Initial Identity Validation.....	14
3.2.1	Method to prove possession of private key	14
3.2.2	Authentication of organization identity.....	14
3.2.3	Authentication of individual identity.....	14

3.2.4	Non-Verified subscriber information.....	14
3.2.5	Validation of authority.....	14
3.2.6	Criteria for interoperation.....	14
3.3	Identification and Authentication for Re-key Requests.....	14
3.3.1	Identification and authentication for routine re-key.....	14
3.3.2	Identification and authentication for re-key after revocation.....	14
3.4	Identification and Authentication for Revocation Requests.....	14
4	Certificate Life-Cycle Operational Requirements.....	14
4.1	Certificate Application.....	14
4.2	Certificate Application Processing.....	15
4.2.1	Performing identification and authentication functions.....	15
4.2.2	Approval or rejection of the certificate applications.....	16
4.2.3	Time to process certificate applications.....	16
4.3	Certificate Issuance.....	16
4.4	Certificate Acceptance.....	16
4.5	Key pair and Certificate Usage.....	16
4.6	Certificate Renewal.....	17
4.7	Certificate Re-key.....	17
4.7.1	Circumstances for certificate re-key.....	17
4.7.2	Who may request certification of a new public key.....	17
4.7.3	Processing certificate re-keying requests.....	17
4.7.4	Notification of new certificate issuance to subscriber.....	17
4.7.5	Conduct constituting acceptance of a re-keyed certificate.....	18
4.7.6	Publication of the re-keyed certificate by the CA.....	18
4.7.7	Notification of certificate issuance by the CA to other entities.....	18
4.8	Certificate Modification.....	18
4.9	Certificate Revocation and Suspension.....	18
4.9.1	Circumstances for revocation.....	18
4.9.2	Who Can Request Revocation.....	18
4.9.3	Procedure for Revocation Request.....	18
4.9.4	Revocation request grace period.....	19
4.9.5	Time within which CA must process the revocation request.....	19
4.9.6	Revocation checking requirement for relying parties.....	19
4.9.7	CRL Issuance Frequency (if applicable).....	19
4.9.8	Maximum latency for CRLs (if applicable).....	19
4.9.9	On-line revocation status checking availability.....	19
4.9.10	On-line revocation checking requirements.....	19
4.9.11	Other forms of revocation advertisements available.....	19
4.9.12	Special requirements re key compromise.....	19

4.9.13	Circumstances for suspension.....	20
4.9.14	Who can request suspension.....	20
4.9.15	Procedure for suspension request	20
4.9.16	Limits on suspension period	20
4.10	Certificate Status Services	20
4.11	End of Subscription	20
4.12	Key Escrow and Recovery	20
5	Management, Operational, and Physical Controls	20
5.1	Physical Security Controls.....	20
5.1.1	Site location and construction.....	20
5.1.2	Physical access.....	20
5.1.3	Power and air conditioning	21
5.1.4	Water exposures	21
5.1.5	Fire prevention and protection	21
5.1.6	Media storage	21
5.1.7	Waste disposal.....	21
5.1.8	Off-site backup.....	21
5.2	Procedural Controls.....	21
5.2.1	Trusted roles	21
5.2.2	Number of persons required per task.....	22
5.2.3	Identification and authentication for each role	22
5.2.4	Roles requiring separation of duties.....	22
5.3	Personnel Security Controls	22
5.3.1	Qualifications, experience, and clearance requirements.....	22
5.3.2	Background check procedures	22
5.3.3	Training requirements.....	22
5.3.4	Retraining frequency and requirements	22
5.3.5	Job rotation frequency and sequence	23
5.3.6	Sanctions for unauthorized actions.....	23
5.3.7	Independent contractor requirements	23
5.3.8	Documentation supplied to personnel	23
5.4	Audit Logging Procedure	23
5.4.1	Types of events recorded	23
5.4.2	Frequency of processing log.....	23
5.4.3	Retention period for audit log.....	23
5.4.4	Protection of audit log.....	24
5.4.5	Audit log backup procedures	24
5.4.6	Audit collection system (internal vs. external).....	24
5.4.7	Notification to event-causing subject.....	24

5.4.8	Vulnerability assessments	24
5.5	Records Archival	24
5.5.1	Types of records archived	24
5.5.2	Retention period for archive.....	24
5.5.3	Protection of archive.....	24
5.5.4	Archive backup procedures	25
5.5.5	Requirements for time-stamping of records	25
5.5.6	Archive collection system (internal or external)	25
5.5.7	Procedures to obtain and verify archive information.....	25
5.6	Key Changeover.....	25
5.7	Compromise and Disaster Recovery	25
5.8	CA or RA Termination	25
6	Technical Security Controls.....	26
6.1	Key Pair Generation and Installation	26
6.1.1	Key pair generation	26
6.1.2	Private Key delivery to subscriber.....	26
6.1.3	Public key delivery to certificate issuer.....	26
6.1.4	CA public key delivery to relying parties.....	26
6.1.5	Key sizes	26
6.1.6	Public key parameters generation and quality checking	26
6.1.7	Key usage purposes (as per X.509 v3 key usage field).....	26
6.2	Private Key Protection and Cryptographic Module Engineering.....	26
6.2.1	Cryptographic module standards and controls	26
6.2.2	Private Key (n out of m) multi person control.....	26
6.2.3	Private Key escrow.....	26
6.2.4	Private Key backup	27
6.2.5	Private Key archival.....	27
6.2.6	Private Key transfer into or from a cryptographic module	27
6.2.7	Private Key storage on cryptographic module	27
6.2.8	Method of activating private key	27
6.2.9	Method of deactivating private key.....	27
6.2.10	Method of destroying private key	27
6.2.11	Cryptographic Module Rating	27
6.3	Other Aspects of Key Pair Management.....	27
6.3.1	Public key archival.....	27
6.3.2	Certificate operational periods and key pair usage periods.....	27
6.4	Activation Data	27
6.5	Computer Security Controls	27
6.5.1	Specific computer security technical requirements.....	27

6.5.2	Computer security rating	28
6.6	Life Cycle Security Controls	28
6.7	Network Security Controls	28
6.8	Time-stamping	28
7	Certificate and CRL Profiles.....	28
7.1	Certificate Profile.....	28
7.1.1	Version number(s).....	28
7.1.2	Certificate Extensions.....	28
7.1.3	Algorithm Object Identifiers.....	29
7.1.4	Name Forms	29
7.1.5	Certificate Policy Object Identifier	30
7.1.6	Usage of Policy Constraints Extensions.....	30
7.1.7	Policy Qualifier Syntax and Semantics.....	30
7.1.8	Processing semantics for the critical Certificate Policies extension.....	30
7.2	CRL Profile.....	30
7.2.1	Version.....	30
7.2.2	CRL and CRL Entry Extensions.....	30
7.3	OCSP Profile.....	30
7.3.1	Version number(s).....	30
7.3.2	OCSP extensions.....	30
8	Compliance Audit and Other Assessment.....	30
8.1	Frequency of Entity Compliance Assessment.....	30
8.2	Identity/Qualifications of Assessor	30
8.3	Assessor's relationship to assessed entity.....	31
8.4	Topics Covered by Assessment	31
8.5	Actions Taken as a Result of Deficiency.....	31
8.6	Communications of Results	31
9	Other Business and Legal Matters	31
9.1	Fees.....	31
9.2	Financial Responsibility.....	31
9.3	Confidentiality of Business Information.....	31
9.4	Privacy of Personal Information.....	31
9.5	Intellectual Property Rights.....	32
9.6	Representations and Warranties	32
9.7	Disclaimers of Warranties.....	32
9.8	Limitations of Liability	32
9.9	Indemnities.....	32
9.10	Term and Termination	32

9.10.1 Term	32
9.10.2 Termination	32
9.10.3 Effect of termination and survival	32
9.11 Individual notices and communications with participants	32
9.12 Amendments	32
9.13 Dispute Resolution Procedures	33
9.14 Governing Law	33
9.15 Compliance with Applicable Law	33
9.16 Miscellaneous Provisions	33
9.17 Other Provisions.....	33
Bibliography.....	33

1 Introduction

1.1 Overview

Center for Development of Advanced Computing (C-DAC) is a Research and Development organization in India. This document is the combined Certificate Policy & Certification Practice Statement of Indian Grid Certification Authority (IGCA). It describes the set of operations and procedures of the certification authority operated by C-DAC, referred as IGCA. This document is structured according to RFC 3647. Sections that are not included have a default value of "No stipulation". The rules & procedures in the document are approved by the IGCA Policy Management Authority (IGCA PMA).

1.2 Document Name and Identification

- Document title:
Indian Grid Certification Authority (IGCA) Certificate Policy and Certification Practice Statement
- Document version: 1.1
- Document date: OCT 2008
- OID:

The following ASN.1 Object Identifier (OID) has been assigned to this document: 1.3.6.1.4.1.31180.10.1.1.0. This OID is constructed as shown in the table below:

IANA	1.3.6.1.4.1
Centre for Development of Advanced Computing	.31180
IGCA	.10
CP/CPS	.1
Major Version	.1
Minor Version	.1

1.3 PKI Participants

1.3.1 Certificate Authorities

The IGCA does not issue certificates to subordinate certification authorities.

1.3.2 Registration Authorities

The IGCA delegates the authentication of individual identity to Registration Authorities (RA). RAs must sign an agreement with the IGCA, stating their adherence to the procedures described in this document. The list of RAs is available from the IGCA website. The following is the IGCA RA registration procedure:

- RA must accept the CP/CPS and agree to all RA responsibilities.

- RA must be an employee of the institution or organization and provide photo ID (passport, PAN card, driver's license or proof of work).
- Complete the RA application form and fax it to IGCA or email scanned copy of application along with photo id to igca@cdacb.ernet.in.
- Send verification e-mail to igca@cdacb.ernet.in.
- IGCA will then arrange face to face meeting with RA.
- RA has to apply for IGCA User certificate.
- After completing the request, IGCA will publish the RA contact information on IGCA website.

1.3.3 Subscribers (End Entities)

IGCA issues certificates for the following subjects:

- Users of GARUDA Grid.
- Foreign collaborators or institutes related to Grid research & scientific collaborations from India.

The term end entity is used to refer to the holder of the private key. For a person certificate it will be the subscriber, but for a host certificate the end entity may be some process running on a machine.

The subscriber is required to:

- Read and adhere to the procedures published in this document.
- Generate a key pair using a trustworthy method.
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
 - for user certificates
 - selecting a pass phrase of at least 12 characters
 - protecting the pass phrase from others
 - always using the pass phrase to encrypt the stored private key
 - never share the private key with other users
 - for host certificates
 - storing them encrypted whenever possible
 - Provide correct information and authorize the publication of the certificate.
 - Use the certificates for the permitted uses only.

1.3.4 Relying parties

IGCA's relying parties include the following:

- Employees of CDAC, research institutes in India or GARUDA Grid Users.
- Foreign collaborators or institutes related to GARUDA Grid research & collaborations.

Relying parties obligations are as follows:

- Must read the procedures published by the IGCA
- Must use the certificates for the permitted uses only.
- Must notify IGCA of any security incidents.

1.3.5 Other participants

No stipulation

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Certificates from IGCA may be used in applications for the following purposes:

- Grid Middleware
- Certificates may also be used to satisfy other general or specific requirements of Grid computing.

1.4.2 Prohibited certificate uses

IGCA certificates should not be used for application that doesn't involve in grid computing activities.

1.5 Policy Administration

1.5.1 Organization administering the document

IGCA is managed by GARUDA Grid Operation center at C-DAC, Knowledge Park, Bangalore.

1.5.2 Contact Details

Contact person for questions related to this document or the IGCA in general:

Dr. Subrata Chattopodhyay

Address:

Centre for Development of Advanced Computing

#1, Old Madras Road, Opp. Aero Engine Division, Byappanhalli, Bangalore 560038

India, Phone: +91-80-25244059, Fax: +91-80-25247724

Email: subratac@cdacb.ernet.in

1.5.3 Person determining CPS suitability for the policy

See section 1.5.2

1.5.4 CPS approval procedures

The IGCA is responsible for the CP and CPS.

For the global grid collaborations, IGCA is a member of APGridPMA.

Major changes must be approved by the APGridPMA Community.

Minor changes can be done by IGCA CA staff & should be notified through APGridPMA mailing list.

1.6 Definitions and Acronyms

1.6.1 General Definitions

The following definitions and associated abbreviations are used in this document.

IGCA

INDIAN Grid Certification Authority.

Certificate Policy (CP)

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

Certification Practice Statement (CPS)

A statement of the practices, which a certificate authority employs in issuing certificates.

Certification Authority (CA)

An entity trusted by one or more users to create and assign public key certificates and are responsible for them during their whole lifetime.

Certificate Revocation List (CRL)

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

Policy qualifier

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

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.

2 Publications and Repository Responsibilities

2.1 Repositories

- The IGCA online repository is available at <http://ca.garudaindia.in>

2.2 Publication of Certificate information

The following information will be published in the repository operated by the IGCA:

- The IGCA's root certificate.

- End entity certificates issued by IGCA.
- A Certificate Revocation List (CRL) issued by IGCA.
- Procedures for each type of IGCA enrollment
- IGCA's signing policy.
- Copy of this CP/CPS.
- Other information related to the IGCA.

2.3 Time or frequency of publication

- Client certificate information, the CA's certificate, and CA's certificate fingerprint will be published in the repository as soon as they are issued.
- The CRL will be published in the repository when it is refreshed on the IGCA
- IGCA enrollment information or this CP/CPS will be published in the repository as they are updated.

2.4 Access Controls on repositories

- The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.
- The IGCA does not impose any access control on the information described in section 2.2.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

Name components vary depending on the type of certificate. Names will be consistent with the name requirements specified in RFC [3280] version 2.

3.1.2 Need for names to be meaningful

The Subject Name in a certificate MUST have a reasonable association with the End Entity.

Each host certificate must be linked to a single network entity.

The common name of the host certificate must be the FQDN of the host.

3.1.3 Anonymity of subscribers

The subscribers cannot be anonymous.

3.1.4 Rules for interpreting various name forms

See section 3.1.2

3.1.5 Uniqueness of Names

The Distinguished Name must be unique for each subject name certified by IGCA.

For a user certificate, the CN must be the full name of the subscriber And combined with subscriber's email id. For a host certificate, the CN must be functional fully qualified domain name.

3.1.6 Recognition, authentication and role of trademarks

No stipulation

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

The IGCA confirms the possession of private key by verification of the CSR signature.

3.2.2 Authentication of organization identity

IGCA verifies the identity of organizations by checking that the organization is known to the grid communities.

3.2.3 Authentication of individual identity

- User: People who request a user certificate will be identified by in person interview with the RA. A photo ID card must be presented at the interview.
- Host: Requests must be authorized as a legal subscriber of the CA and RA's approval is required before issuing host certificates for a proof of the subscriber's title of the host FQDN.

3.2.4 Non-Verified subscriber information

No stipulation.

3.2.5 Validation of authority

No Stipulation

3.2.6 Criteria for interoperation

No Stipulation

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key

See section 4.7.2

3.3.2 Identification and authentication for re-key after revocation

Rekey after revocation follows the same rules as an initial registration.

3.4 Identification and Authentication for Revocation Requests

Use the CRIN (Certificate Revocation Number) pin mailed to the user during the issue of the certificate or contact the igca@cdacb.ernet.in using signed email to verify his/her identity.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Enrollment process for user certificate as follows:

- A user who requests for user certificate must have a face-to-face meeting with the RA and present a filled user application form to RA. (The application form can be downloaded from IGCA website). Along with application form, the user has to attach his photo identity (passport, driver's license, pan card or proof of work). Note, the subscriber has to specify his Certificate Request **Serial no** in the user application (this is obtained from the next step).
- Note, this step has to be completed before the Face to Face meeting with RA. The user goes online and requests for CSR. The key generation happens at the client side.
- The RA examines the request according to section 3.2.
- Once the user is identified, the RA will put the signature on the user application form.
- The user will fax or email the scanned copy of the application form to igca@cdacb.ernet.in.
- Upon receipt of the application form, the IGCA manager will verify the RA signature in the application form, making sure that the RA has really signed it. The IGCA manager can contact the RA if necessary via signed e-mail or telephone. IGCA Manager will verify the CSR no.
- Now the CA operator (CAO) will issue the certificate and sends an email regarding the downloading of the his/her certificates.

Enrollment process for host certificate as follows:

- A user who requests for host certificate must be an existing subscriber of IGCA.
- A user who requests for host certificate must have a face-to-face meeting with the RA and present a filled host application form to RA. (The application form can be downloaded from IGCA website). Along with application form, the user has to attach his photo identity (passport, driver's license, pan card or proof of work). Note, the subscriber has to specify his User Certificate **serial no**. in the host application form.
- Generate a CSR on client machine and upload the CSR to the IGCA web server through web browser and note down the **Serial No** and fill in the application form.
- The RA examines the request according to section 3.2.
- Once the user is identified, the RA will put the signature on the host application form.
- The user will fax or email the scanned copy of the application form to igca@cdacb.ernet.in.
- Upon receipt of the application form, the IGCA manager will verify the RA signature in the application form, making sure that the RA has really signed it. The IGCA manager can contact the RA if necessary via signed e-mail or telephone. IGCA Manager will verify the user certificate serial no.
- Now the CA operator (CAO) will issue the certificate and sends an email regarding the downloading of the host certificates.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

In the enrollment process, the IGCA manager checks if

- The application form is correct; and
- If, RA examined the subscriber in a face-to-face meeting.

In the certificate application process, the IGCA manager checks if

- The certificate request is done in accordance with the process in this document especially in the section 4.1
- The certificate request subject name has correct format; and
- The key length of the certificate request meets the requirement

4.2.2 Approval or rejection of the certificate applications

- The issuance of a certificate by the CA indicates a complete and final approval of the certificate application by the CA.
- If any condition specified in section 4.2.1 is not satisfied, the certificate application is rejected and the CA notifies to the subscriber with reason of the rejection.

4.2.3 Time to process certificate applications

- The CA should process the certificate application within 3 working days from the acceptance of the certificate request.

4.3 Certificate Issuance

- Upon the receipt of CSR, the CAO will store the CSR in a dedicated pendrive and take it to the IGCA signing machine, which is kept off-line as described in 6.7.
- The CAO generates (issues) user certificate containing user public key with CA signature and hand-carrying it to the online public web server.
- A notification message is sent to the e-mail address of the subscriber with the instructions on how to download it from the online public web server.
- The user will be able to download his/her user certificate. For this secure http connection is required.
- If the authentication is not successful, the certificate is not issued and an e-mail with reason is sent to the subscriber.

4.4 Certificate Acceptance

- If the issued certificate has any problem, the subscriber should notify the CA that he/she can not accept the issued certificate with a proper reason within 7 days from the issuance of the certificate.
- Unaccepted certificate should be revoked & the certificate should be re-issued.

4.5 Key pair and Certificate Usage

- IGCA certificate can be used for any software for grid computing.
- User certificate must not be shared with multiple people.
- Host certificate must be linked to a single network entity.
- The subscriber should manage his certificates and private keys securely. To protect the private key, the subscriber must encrypt private key with a pass phrase. The pass phrase should be minimum of 12 characters long.

4.6 Certificate Renewal

IGCA does not permit certificate signing request with the same key as the previous certificate.

4.7 Certificate Re-key

4.7.1 Circumstances for certificate re-key

Generally, certificate re-key can or must take place in cases such as:

Case 1: after a certificate is revoked for reasons of key compromise; or

Case 2: after a certificate has expired.

Case 3: one (1) month prior to the expiration of the certificate.

4.7.2 Who may request certification of a new public key

- A subscriber of IGCA can request certification of a new public key in the following conditions.
- If a certificate of the subscriber is revoked for reasons of key compromise (case 1 in section 4.7.1).
- If a certificate has expired (case 2 in sections 4.7.1).
- If a certificate is going to be expired in one month (case 3 in section 4.7.1)

4.7.3 Processing certificate re-keying requests

- If a certificate is revoked for reasons of key compromise (case 1 in section 4.7.1):
 - The compromised certificate must be revoked and the subscriber of the certificate should follow the enrolment process (section 4.1), again to get a new certificate.
- If a certificate has expired (case 2 in section 4.7.1):
 - The expired certificate must be revoked and the subscriber of the certificate should follow section 4.1 to get a new certificate.
- If a certificate expires in one (1) month (case 3 in section 4.7.1):
 - The subscriber, who has valid certificate, need not fill the application form and need not participate in the Face-to-Face meeting with RA until 5 years of initial ID vetting. After 5 years the subscriber of the certificate should follow the enrolment process (section 4.1), again to get a new certificate.
 - Request for the rekey using the online request form and send a signed email to igca@cdacb.ernet.in (Use your user certificate to send signed email).
 - In the email, the subscriber has to mention the current certificate serial no. and newly rekey Certificate Signing Request (CSR) number.
 - If a subscriber applies to rekey his/her certificate prior to the expiration of previous certificate, CAO should revoke the previous certificate within 1 week after issuing the new certificate but not after the expiration time of the old certificate.
 - IGCA does not permit certificate signing request with the same key as the previous certificate. The new certificate request must use a different key with the previous certificate

4.7.4 Notification of new certificate issuance to subscriber

- Basically same as the initial certificate issuance in the section 4.1.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

- Basically same as the initial certificate issuance in the section 4.1.

4.7.6 Publication of the re-keyed certificate by the CA

- Basically same as the initial certificate issuance in the section 4.1.

4.7.7 Notification of certificate issuance by the CA to other entities

- Basically same as the initial certificate issuance in the section 4.1.

4.8 Certificate Modification

- IGCA doesn't support certificate modification

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

A certificate must be revoked when information it contains is suspected to be incorrect or compromised. This includes situations where:

- The subscriber's private key is compromised or is suspected to have been compromised.
- The subscriber's information in the certificate is suspected to be inaccurate.
- An end entity must request revocation of its certificate as soon as possible but within one working day after detection of key compromise/the data in the certificate are no longer valid.
- The subscriber is known to have violated his obligations, which could induce a critical security hole.
- The subscriber leaves his/her organization.
- In case of host certificates, the corresponding host is retired.

4.9.2 Who Can Request Revocation

IGCA will accept a revocation request made by

- The certificate subscriber
- RA
- CA and
- Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key

4.9.3 Procedure for Revocation Request

Entities requesting revocation of a certificate must authenticate themselves in one of the following ways:

Subscriber requesting revocation:

- Use the CRIN pin and fill the online revocation request. Send a confirmation email signed by a valid and trusted certificate to igca@cdacb.ernet.in.
- In case if u lost CRIN pin request for CRIN pin by sending a signed email to igca@cdacb.ernet.in .

RA

- RA can request for revocation if subscriber leaves the organization or finds any unusual certificate. Send signed email to igca@cdacb.ernet.in with the subscriber details.

In all the above cases, the requesting entity must specify the reason for the revocation request and provide evidence of circumstances as described in section 4.9.1.

4.9.4 Revocation request grace period

- CA will process revocation as soon as it receives the revocation request and the request is approved.
- The revocation information will be published to the online repository.
- During the revocation, a revocation notification is sent to the subscriber's email.

4.9.5 Time within which CA must process the revocation request

The CA should process the certificate revocation request within 1 working day from the recognition of the request.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL Issuance Frequency (if applicable)

- The lifetime of the CRL is 30 days.
- A new CRL is issued immediately after a revocation or at least 7 days before expiration.

4.9.8 Maximum latency for CRLs (if applicable)

- CRLs must be published in the repository after generation as soon as possible.
- In IGCA, the maximum latency between the generation of CRLs and posting of the CRLs to the repository is 1 hour.

4.9.9 On-line revocation status checking availability

IGCA system does not provide any online status checking facility.

4.9.10 On-line revocation checking requirements

IGCA system does not provide any online status checking facility.

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

IGCA does not support Certificate Suspension.

4.9.14 Who can request suspension

IGCA does not support Certificate Suspension.

4.9.15 Procedure for suspension request

IGCA does not support Certificate Suspension.

4.9.16 Limits on suspension period

IGCA does not support Certificate Suspension.

4.10 Certificate Status Services

IGCA support only status like requested certificate, valid certificates, and revoked certificates.

4.11 End of Subscription

If a subscriber of IGCA end the subscription to the CA services:

The subscriber must do the following:

- Must not use any certificate issued from IGCA
- Must delete his private key from his web browser.

The CA must do the following:

- Must revoke all certificates issued for the subscriber.

4.12 Key Escrow and Recovery

No stipulation.

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

The CA operates in a controlled environment, where access is restricted to authorized people.

5.1.1 Site location and construction

IGCA is located at C-DAC, Knowledge Park, Bangalore, India.

5.1.2 Physical access

Physical access to the CA machine is restricted to authorized personnel. All events about the access to the room should be recorded. The IGCA machines (both the issuing machine and the public web server) are:

- Running on dedicated machines.
- Located in a secure environment where access is controlled.

5.1.3 Power and air conditioning

The CA signing machine and the CA web server are both protected by uninterruptible power supplies. Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by suitable air conditioning systems.

5.1.4 Water exposures

The CA shall ensure that the CA system is adequately protected from water exposures.

5.1.5 Fire prevention and protection

The building housing IGCA facilities has a fire alarm system. The IGCA shall ensure that the CA system is adequately protected from fire by a fire suppression system.

5.1.6 Media storage

The CA private key and backup copies of CA related information is securely kept in several removable storage media.

5.1.7 Waste disposal

The CA shall ensure that all media containing sensitive information is sanitized, to remove information such that data recovery is not possible, or destroyed before release for disposal. CA personnel shall account for the destruction of sensitive information.

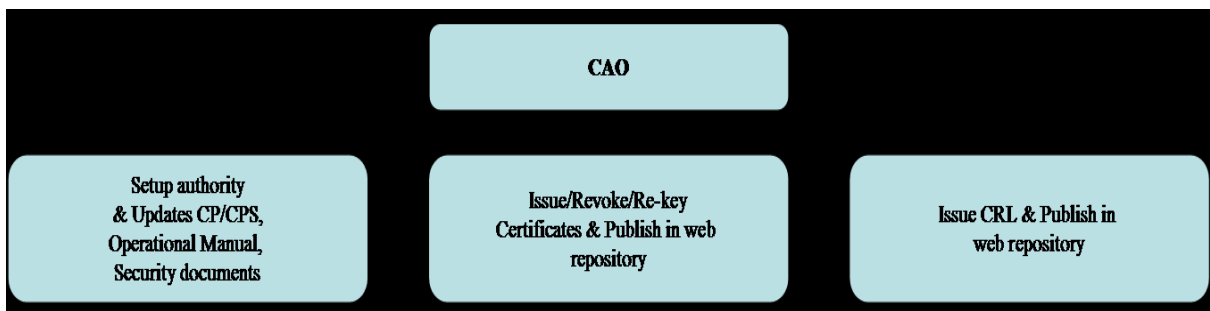
5.1.8 Off-site backup

In IGCA, no off-site backups are currently performed.

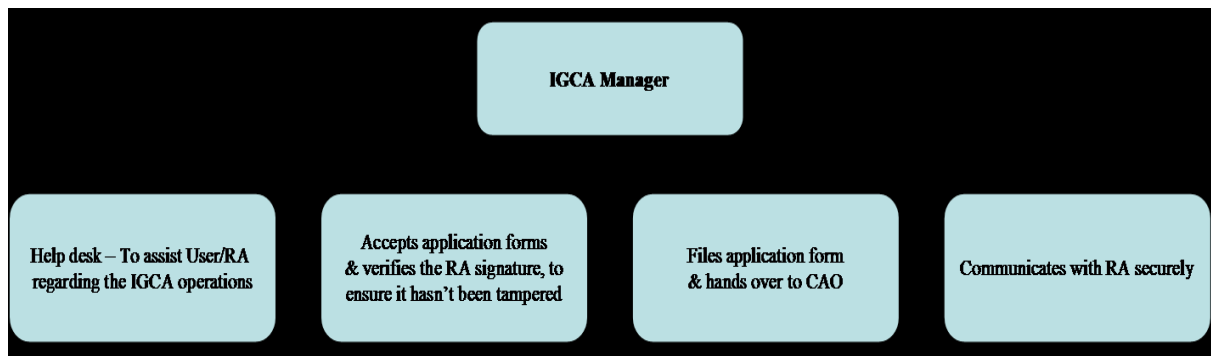
5.2 Procedural Controls

5.2.1 Trusted roles

- CERTIFICATE AUTHORITY OPERATOR (CAO) can manage all system related activities, certificates, requests and cryptographic data including CA private key. CAO is contact point for subscribers about CA operation. CAO can make changes of CP/CPS. Only CAO can issue/revoke certificate and issue CRL.



- IGCA Manager examines subscriber's information and checks RA signature to ensure that it hasn't been tampered. Then later CAO will issue the certificate.



- SYSTEM AUDITOR has read-only access to all components of the PKI system to verify the operation complies with the rules and regulations of this CP/CPS.

5.2.2 Number of persons required per task

For operation of IGCA, the number of persons required for the roles is:

- CERTIFICATE AUTHORITY OPERATOR: 3 persons.
- IGCA MANAGER: 2 persons.
- SYSTEM AUDITOR: 1 person.

5.2.3 Identification and authentication for each role

In IGCA, on-line and/or off-line system will identify and authenticate the operator when the staff operates the system.

5.2.4 Roles requiring separation of duties

- SYSTEM AUDITOR may not be a CERTIFICATE AUTHORITY OPERATOR.

5.3 Personnel Security Controls

All access to the servers and applications that comprise the IGCA PKI is limited to IGCA security staffs.

5.3.1 Qualifications, experience, and clearance requirements

The IGCA shall ensure that all staff performing CA and RA functions possesses the necessary knowledge, experience and qualifications to perform their duties.

5.3.2 Background check procedures

CA personnel must be a formal member of IGCA.

5.3.3 Training requirements

The CA shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as security requirements, operational responsibilities and associated procedures.

5.3.4 Retraining frequency and requirements

The IGCA shall review and update its training program at least once a year to accommodate changes in the CA system.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized actions by a person performing duties with respect to the operation of the CA or an RA, the IGCA shall suspend his or her access to the CA system.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

The IGCA shall provide these Certificate Policies, relevant provisions of the CPS to CA personnel, RAs.

5.4 Audit Logging Procedure

- The IGCA will retain records as much as possible so that the IGCA could trace anything if something illegal would happen.
- Such audit information is not publicly available.
- Auditors are allowed to access the information as part of auditing and such information must be kept confidential.
- CA operator performs operational audits of the IGCA Manager/RA staff at least once per year.

5.4.1 Types of events recorded

- Certification requests
- Revocation requests
- Issued certificates
- Issued CRLs
- Shutdown/boot/reboot/login/logout/sudo logs of the CA machine and on-line request web server.
- Other logs archived by UNIX operating system of the CA machine and RA server

5.4.2 Frequency of processing log

The IGCA shall ensure that all significant events are explained in an audit log summary and that CA personnel review audit logs at least once every month. Such reviews involve verifying that the log has not been tampered with, and then inspecting all log entries. CA personnel shall conduct a more thorough investigation of any "alerts" or irregularities in the logs. The IGCA shall indicate who has responsibility for audit log review and audit log summary preparation in the CPS.

5.4.3 Retention period for audit log

The IGCA shall retain its audit logs on site for at least two (2) months and subsequently retain audit logs in the manner described in section 5.5.

5.4.4 Protection of audit log

The IGCA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 Audit log backup procedures

The IGCA shall back up or copy all audit logs and audit summaries.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

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

- CA's records archival
 - CA records all the types of events listed in section 5.4.1 are archived.
 - In addition to that, email sent to/from igca@cdacb.ernet.in messages will be archived as well.
 - CA private keys must be backed up and protected at a level of physical and cryptographic protection equal to or exceeding that in place at the CA site.
- RA's records archival
 - RA records all the types of events regarding user registration, certificate/revocation request including:
 - date of meeting with a subscriber
 - evidence of identity of a subscriber
 - Email messages sent to/from the RA's email address.

5.5.2 Retention period for archive

Certificates and CRLs generated by the CA must be retained for at least 3 years after their expiration, and;

The minimum retention period is 3 years.

5.5.3 Protection of archive

System logs and email archives are protected by the authorization mechanism provided by Unix operating system. Only the owners of the system logs are able to modify the logs. System logs and email archives are periodically back-up to the offline media, which is stored in a safe place.

5.5.4 Archive backup procedures

A second copy of all material retained or backed up must be stored in read-only media like CD-ROM.

The second copy must be protected either by physical security alone, or a combination of physical and cryptographic protection.

5.5.5 Requirements for time-stamping of records

All archived logs and documents are time stamped.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key Changeover

- When the CA's cryptographic data needs to be changed (e.g. CA key expiration), from the time of distribution of new cryptographic data, only the new CA certificate will be used for certificate signing purposes.
- From that time, the old CA certificate will not be used for certificate signing purposes.
- The overlap of the old and new CA certificate must be at least the longest time an end-entity certificate can be valid (1 year).
- The old CA certificate will be valid and available to verify old signatures and the secret key to sign CRLs until all the certificates signed using the associated private key have also expired.
- The life of CA certificate will be 10 years.

5.7 Compromise and Disaster Recovery

- If it is detected that hardware, software or data are corrupted or damaged
 - Recover the system by using backup hardware, software, or data as quickly as possible.
- If a CA's private key is compromised or suspected to be compromised, the IGCA will:
 - Notify subscribers, RAs and relying parties.
 - Revoke all issued certificates.
 - Terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key.
 - Create a new pair of key and re-build the CA system.

5.8 CA or RA Termination

Before IGCA terminates its services it will:

- Make publicly available information of its termination.
- Stop issuing certificates and CRLs.
- Destroy its private key's and all copies.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

- A CA key pair is generated by CA staff on a signing machine, which is not connected to any kind of network.
- End entities' cryptographic keys are locally generated by their application during the requesting process.
- IGCA does not generate private keys for subjects.

6.1.2 Private Key delivery to subscriber

The IGCA does not generate end entities private keys hence does not deliver private keys. User's private key could be generated by browser application in personal computer.

6.1.3 Public key delivery to certificate issuer

End entity will send its public key included in CSR at time of certificate request.

6.1.4 CA public key delivery to relying parties

CA certificate will be published on the IGCA repository.

6.1.5 Key sizes

- The minimum key length for user or host certificate is 1024 bits.
- The CA key length is 2048 bits.

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)

IGCA private key is the only key used for signing CRLs and Certificates for end entity certificates.

6.2 Private Key Protection and Cryptographic Module Engineering

6.2.1 Cryptographic module standards and controls

IGCA do not use any hardware security module.

6.2.2 Private Key (n out of m) multi person control

In IGCA system, (n out of m) multi-person control is not supported.

The pass phrase for accessing to CA's private key is known to 3 CA Operators.

6.2.3 Private Key escrow

Not supported.

6.2.4 Private Key backup

The IGCA private key backup is performed by CA operator and the two copies of backup key is kept encrypted in a CDROM and dedicated pendrive respectively in a safe place where access is controlled.

6.2.5 Private Key archival

See section 5.5.

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

See section 6.4.

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 IGCA shall retain all public key certificates it generates.

6.3.2 Certificate operational periods and key pair usage periods

- The lifetime of IGCA certificate is ten (10) years.
- The lifetime of user certificate is one (1) year.
- The lifetime of host certificate is one (1) year.

6.4 Activation Data

- The IGCA's private key is protected by a pass phrase with a minimum 15 characters.
- This pass phrase is only known by CA operators.
- The pass phrase is in a sealed envelope kept in a safe place where access is controlled.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

- CA operating systems are maintained at a high level of security by applying all the relevant patches.
- Monitoring is performed to detect unauthorized software changes.

- CA systems configuration is reduced to the base minimum.
- Both CA signing machine and web server machine are used for dedicated purpose respectively.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

- The CA signing machine is kept off-line.
- The CA web server machine is protected by a firewall.
- The CA web server machine is a dedicated machine and only required services run on the server.
- Appropriate software upgrade/patch of the CA web server is performed every 6 month or immediately if it is required.

6.8 Time-stamping

No stipulation.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

X.509 v3.

7.1.2 Certificate Extensions

CA Certificate:

X509v3 Basic Constraints	Critical, CA: TRUE
X509v3 Key Usage	Critical, Certificate Sign (keyCertSign), CRL Sign (cRLSign)
X509v3 Subject Key Identifier	[the unique Key ID]
X509v3 Authority Key Identifier	keyid
X509v3 Subject Alternative Name	Email: igca@cdacb.ernet.in
X509v3 Issuer Alternative Name	Email: igca@cdacb.ernet.in

User Certificate:

X509v3 Basic Constraints	critical CA:FALSE
X509v3 Key Usage	critical, Digital Signature (digitalSignature), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
extendedKeyUsage	clientAuth
X509v3 Subject Key Identifier	[the unique Key ID]
X509v3 Authority Key Identifier	keyid
X509v3 Issuer Alternative Name	Email: igca@cdacb.ernet.in
X509v3 Subject Alternative Name	Email : subscriber email ID
X509v3 Certificate Policies policyIdentifier	1.3.6.1.4.1.31180.10.1.1.1
policyIdentifier	1.2.840.113612.5.2.2.1
X509v3 CRL Distribution Points	<i>URL of CRL</i>

Host Certificate:

X509v3 Basic Constraints	critical CA:FALSE
X509v3 Key Usage	critical, Digital Signature (digitalSignature), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
extendedKeyUsage	serverAuth, clientAuth
X509v3 Subject Key Identifier	[the unique Key ID]
X509v3 Authority Key Identifier	keyid
X509v3 Issuer Alternative Name	Email: igca@cdacb.ernet.in
X509v3 Certificate Policies policyIdentifier	1.3.6.1.4.1.31180.10.1.1.1
policyIdentifier	1.2.840.113612.5.2.2.1
X509v3 Subject Alternative Name	DNS: [FQDN of the host]
X509v3 CRL Distribution Points	<i>URL of CRL</i>

7.1.3 Algorithm Object Identifiers

Signature Algorithm: sha1WithRSAEncryption (2048 bits)

7.1.4 Name Forms

- Issuer:

DC=IN, DC=GARUDAINDIA, CN=Indian Grid Certification Authority

- Person DN:
DC=IN, DC=GARUDAINDIA, O=C-DAC, OU=CTSF, CN=<Applicants Name> (EmailAddress)
- Host DN:
DC=IN, DC=GARUDAINDIA, O=C-DAC, OU=CTSF, CN=<FQDN of server>

7.1.5 Certificate Policy Object Identifier

See section 1.2.

7.1.6 Usage of Policy Constraints Extensions

No Stipulation.

7.1.7 Policy Qualifier Syntax and Semantics

No Stipulation.

7.1.8 Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2 CRL Profile

CRLs are signed by the IGCA private key and are published in a web page.

7.2.1 Version

x.509 v2.

7.2.2 CRL and CRL Entry Extensions

Message digest algorithm of the CRL: SHA-1

7.3 OCSP Profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 Compliance Audit and Other Assessment

8.1 Frequency of Entity Compliance Assessment

The IGCA will accept external Compliance Audit.

In addition, the IGCA performs operational self-assessment of CA/RA staff at least once per year.

8.2 Identity/Qualifications of Assessor

IGCA can be audited by the APGrid PMA.

8.3 Assessor's relationship to assessed entity

IGCA can be audited by the APGrid PMA.

8.4 Topics Covered by Assessment

Audit items will be selected based on the minimum CA requirements and documents enacted by the APGridPMA.

8.5 Actions Taken as a Result of Deficiency

The IGCA has the responsibility for the action to be taken as a result of deficiency. When the IGCA receives an audit report from the auditor, it will send a report on actions to the auditor within two weeks.

The report must describe actions taken as a result of deficiency and their timetable.

8.6 Communications of Results

The result of the audit will be made available to APGrid PMA in which the IGCA participates. It may make the results of the audit publicly available.

9 Other Business and Legal Matters

9.1 Fees

No fees are charged for any service provided by the IGCA.

9.2 Financial Responsibility

Accept no liability at all.

9.3 Confidentiality of Business Information

- IGCA collects subscriber's full names and email addresses. Some of this information is used to construct unique, meaningful subject names in the issued certificates.
- Information included in issued certificates and CRLs is not considered confidential.
- IGCA does not collect any kind of confidential information.
- IGCA does not have access to or generate the private keys of a digital signature key pair, such as those used in IGCA identity certificates. These key pairs are generated and managed by the subscribers and are the sole responsibility of the subscribers.

9.4 Privacy of Personal Information

The subscriber's private information collected for registration are:

- Name of subscriber
- Organization Name
- Telephone
- Email

We do not provide this information to other organizations.

9.5 Intellectual Property Rights

All certificate related data issued by IGCA is not under any copyright or intellectual property protection.

9.6 Representations and Warranties

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

- IGCA issues person certificates according to the practices described in this document.
- IGCA makes no guarantee about the security or suitability of a service that is identified by an IGCA certificate.
- The certification service is run with a reasonable level of security, but it is provided on a best effort only basis.
- It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.
- IGCA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP/CPS is valid and enforceable from the time of accreditation by APGrid PMA.

9.10.2 Termination

This CP/CPS terminates in the following cases:

- CA certificate expires
- CA terminates its service
- A new version of CP/CPS is accredited.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

- Users will not be warned in advance of changes to the IGCA's policy and CPS.

- Any revision of specification is made by IGCA PMA and it is approved by the APGridPMA.
- Minor editorial changes to this document can be made without approval by the APGridPMA.
- New OID will not be assigned to the revised document when minor changes would be made.
- Major changes such as changes in policy or technical security controls need to be approved by the APGrid PMA. New OID will be assigned to the revised document for such major changes would be made.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

IGCA is subject Indian Law.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.

Bibliography

CERN CA

CERN CA Certificate Policy and Certification Practice Statement.
<http://home.cern.ch/globus/ca/CPS.pdf>

DATAGRID-ES CA

DATAGRID-ES CA Certificate Policy and Certification Practice Statement.
<http://www.ifca.unican.es/datagrid/ca/datagrid-ca-policy.doc>

DOE Grid PKI

DOE Science Grid PKI Certificate Policy and Certification Practice Statement Version 2.1.
<http://www.doe grids.org/Docs/CP-CPS.pdf>

INFN CA

INFN CA Certificate Policy and Certification Practice Statement
<http://security.fi.infn.it/CA/CPS/CPS-2.2.pdf>

RFC 3280

<http://www.ietf.org/rfc/rfc3280.txt>

RFC 3647

<http://www.ietf.org/rfc/rfc3647.txt>

References

- [1] Academia Sinica Grid Computing Certification Authority (ASGCCA) Certificate Policy and Certification Practice Statement, OID: 1.3.6.1.4.1.5935.10.1.1.1, June 2003.
- [2] NAREGI Certification Practice Statement Ver1.0.1, OID:1.2.392.00200181.1.1, September 27, 2005
- [3] AIST GRID PKI Service Certificate Policy and Certificate Practice Statement Ver.1.1.1, CP OID:1.3.6.1.4.1.18936.1.11.2 and CPS OID:1.3.6.1.4.1.18936.1.11.1, June 15, 2005