

CNIC Grid CA  
Certificate Policy  
And  
Certification Practice Statement  
Version 1.2

DN: CN=Root Certificate Authority at CNIC,DC=Grid,DC=CN

**Computer Network Information Center,  
Chinese Academy of Sciences  
(CNIC, CAS)**

July 18, 2006

## Version History

Version	Author	Participator	Date	Comment
1.0	Morrise Xu	CNIC Grid CA PMA	2005-12-31	Initial Document
1.1	Morrise Xu	CNIC Grid CA PMA	2006-5-11	Refer to the CESNET CA CP/CPS
1.2	Morrise Xu	APGrid PMA	2006-7-18	Reviewed by the APGrid PMA

# Index

1 Introduction .....	7
<b>1.1 Overview</b> .....	7
1.1.1 Type of Certificates .....	7
1.1.2 Related specification .....	7
<b>1.2 Identification</b> .....	7
<b>1.3 Community and Applicability</b> .....	8
1.3.1 Organization .....	8
1.3.2 Certification Authorities .....	9
1.3.3 Registration Authorities .....	9
1.3.4 End Entities .....	9
1.3.5 Applicability .....	9
1.3.6 User Restriction .....	9
<b>1.4 Contact Details</b> .....	9
1.4.1 Specification administration organization .....	9
1.4.2 Contact Person .....	9
2 General Provisions .....	10
<b>2.1 Obligations</b> .....	10
2.1.1 CA Obligations .....	10
2.1.2 RA Obligations .....	10
2.1.3 Subscriber Obligations .....	11
2.1.4 Relying Party Obligations .....	11
2.1.5 User Administrator Obligations .....	11
2.1.6 Repository Obligations .....	12
<b>2.2 Liability</b> .....	12
2.2.1 CA liability .....	12
2.2.2 RA liability .....	12
2.2.3 Certificate Users and host administrators liability .....	12
2.2.4 Relying party liability .....	12
2.2.5 User Administrator liability .....	12
2.2.6 Repository liability .....	13
<b>2.3 Financial Responsibility</b> .....	13
<b>2.4 Interpretation and Enforcement</b> .....	13
2.4.1 Governing Law .....	13
2.4.2 Serverability, survival, merge, notice .....	13
2.4.3 Dispute resolution procedures .....	13
<b>2.5 Fees</b> .....	13
<b>2.6 Publication and Repositories</b> .....	13
2.6.1 Publication of CA information .....	13
2.6.2 Frequency of Publication .....	14
2.6.3 Access Controls .....	14
2.6.4 Repositories .....	14
<b>2.7 Compliance Audit</b> .....	14

2.7.1	Frequency of Entity Compliance Audit .....	14
2.7.2	Identity/Qualifications of Auditor .....	14
2.7.3	Auditor's Relationship to Audited Party .....	15
2.7.4	Topics Covered by Audit .....	15
2.7.5	Actions taken as a result of deficiency .....	15
2.7.6	Communication of results .....	15
2.8	<b>Confidentiality</b> .....	15
2.8.1	Types of information to be kept confidential .....	15
2.8.2	Information Considered Not Confidential .....	15
2.8.3	Disclosure of certificate revocation/suspension information .....	16
2.8.4	Release to law enforcement officials .....	16
2.8.5	Release as part of civil discovery .....	16
2.8.6	Disclosure upon owner's request .....	16
2.8.7	Other information release circumstances .....	16
2.9	<b>Intellectual Property Rights</b> .....	16
3	<b>Identification and Authentication</b> .....	16
3.1	<b>Initial Registration</b> .....	16
3.1.1	Types of names .....	16
3.1.2	Name Meanings .....	17
3.1.3	Rules for Interpreting Various Name Forms .....	17
3.1.4	Uniqueness of Names .....	17
3.1.5	Name Claim Dispute Resolution Procedure .....	17
3.1.6	Recognition, Authentication, and Role of Trademarks .....	17
3.1.7	Method to Prove Possession of Private Key .....	17
3.1.8	Authentication of Organization Identity .....	18
3.1.9	Authentication of Individual Identity .....	18
3.2	<b>Routine Rekey</b> .....	18
3.3	<b>Rekey After Revocation</b> .....	18
3.4	<b>Revocation Request</b> .....	18
4	<b>Operational Requirements</b> .....	19
4.1	<b>Certificate Application</b> .....	19
4.2	<b>Certificate Issuance</b> .....	19
4.2.1	Receipt Certificate Enrollment .....	19
4.2.2	Insurance Certificate .....	20
4.2.3	Subscribe Certificate .....	20
4.3	<b>Certificate Acceptance</b> .....	20
4.4	<b>Certificate Suspension and Revocation</b> .....	20
4.4.1	Circumstances for Revocation .....	20
4.4.2	Who Can Request Revocation .....	21
4.4.3	Procedure for Revocation Request .....	21
4.4.4	Revocation Request Grace Period .....	21
4.4.5	Circumstances for Suspension .....	21
4.4.6	Who Can Request Suspension .....	21
4.4.7	Procedure for Suspension Request .....	21

4.4.8 Limits on Suspension Period .....	22
4.4.9 CRL Issuance Frequency.....	22
4.4.10 CRL Checking Requirements for Relying Parties .....	22
4.4.11 Online Revocation/Status Checking Availability .....	22
4.4.12 Online Revocation Checking Requirements .....	22
4.4.13 Other Forms of Revocation Advertisement Available .....	22
<b>4.5 Security Audit Procedures .....</b>	<b>22</b>
4.5.1 Types of event recorded.....	22
4.5.2 Frequency of processing log.....	23
4.5.3 Retention period for audit log .....	23
4.5.4 Protection of audit log .....	23
4.5.5 Audit log backup procedures .....	23
4.5.6 Audit collection system (internal vs external) .....	23
4.5.7 Notification to event-causing subject.....	23
4.5.8 Vulnerability assessments.....	24
<b>4.6 Records Archival .....</b>	<b>24</b>
4.6.1 Types of Event Audited .....	24
4.6.2 Retention Period for Audit Logs .....	25
4.6.3 Protection of Archive.....	25
4.6.4 Archive Backup Procedures .....	25
4.6.5 Time-Stamping Requirements.....	25
4.6.6 Archive Collection System .....	25
4.6.7 Procedures to Obtain and Verify Archive Information.....	25
<b>4.7 Key Changeover .....</b>	<b>25</b>
<b>4.8 Compromise and Disaster Recovery .....</b>	<b>25</b>
<b>4.9 CA Termination.....</b>	<b>26</b>
<b>5 Physical, Procedural and Personnel Security Controls.....</b>	<b>26</b>
<b>5.1 Physical Security Controls .....</b>	<b>26</b>
5.1.1 Site Location.....	26
5.1.2 Physical Access.....	26
5.1.3 Power and Air Conditioning .....	27
5.1.4 Water Exposure .....	27
5.1.5 Fire Prevention and Protection.....	27
5.1.6 Media Storage.....	27
5.1.7 Waste Disposal .....	27
5.1.8 Off-site Backup .....	27
<b>5.2 Procedural Controls .....</b>	<b>27</b>
5.2.1 Trusted roles .....	27
5.2.2 Number of persons required per task.....	28
5.2.3 Identification and authentication for each role .....	28
5.2.4 Roles requiring separation of duties .....	28
<b>5.3 Personnel Security Controls .....</b>	<b>28</b>
<b>6 Technical Security Controls .....</b>	<b>28</b>
<b>6.1 Key Pair Generation and Installation.....</b>	<b>28</b>

6.1.1 Key Pair Generation.....	28
6.1.2 Private Key Delivery to Entity .....	28
6.1.3 Public Key Delivery to Certificate Issuer.....	29
6.1.4 CA Public Key Delivery to Users.....	29
6.1.5 Key Sizes.....	29
6.1.6 Public Key Parameters Generation .....	29
6.1.7 Parameter Quality Checking.....	29
6.1.8 Hardware/Software Key Generation.....	29
6.1.9 Key Usage Purposes .....	29
<b>6.2 Private Key Protection.....</b>	<b>29</b>
6.2.1 Private Key (n out of m) Multi-person Control.....	29
6.2.2 Private Key Escrow .....	30
6.2.3 Private Key Archival and Backup.....	30
<b>6.3 Other Aspects of Key Pair Management .....</b>	<b>30</b>
<b>6.4 Activation Data .....</b>	<b>30</b>
<b>6.5 Computer Security Controls.....</b>	<b>30</b>
6.5.1 Specific Computer Security Technical Requirements.....	30
6.5.2 Computer Security Rating.....	30
<b>6.6 Life-Cycle Security Controls .....</b>	<b>30</b>
<b>6.7 Network Security Controls .....</b>	<b>30</b>
<b>6.8 Cryptographic Module Engineering Controls.....</b>	<b>31</b>
7 Certificate and CRL Profiles .....	31
7.1 Certificate Profile .....	31
7.2 CRL Profile.....	31
8 Specification Administration.....	31
8.1 Specification Change Procedures.....	31
8.2 Publication and Notification Procedures .....	31
8.3 CPS Approval Procedures.....	31
Glossary.....	31
Bibliography.....	33
Appendix A. Change Logs.....	34

# 1 Introduction

This document is based on the structure suggested by the RFC 2527. Not all sections of RFC 2527 are used. Sections that are not included have a default value of "No Stipulation".

This document describes the set of rules and procedures established by CNIC for the operations of the CNIC Grid Root CA service.

Now CNIC Grid CA has only one Root CA.

The terms used in this document are explained in the Glossary.

## 1.1 Overview

This document describes the set of rules and procedures followed by CNIC Grid Certificate Authority (CNIC Grid CA), the top level CA for all purposes of *Grid research* in CNIC.

### 1.1.1 Type of Certificates

CNIC Grid CA issues following types of certificates:

- Subordinate CA certificates
- User certificates which will be used for CNIC Grid CA/RA administrator
- Host certificates which will be used for CNIC Grid CA/RA Server

### 1.1.2 Related specification

None.

## 1.2 Identification

Document Title

**CNIC Grid CA Certificate Policy and Certification Practice Statement**

Document Version **1.2**

Document Date **Dec 31, 2005**

Last Update Date **July 18, 2006**

CP OID: 1.3.6.1.4.1.8728.2.2.2.1.1.1.2

CPS OID: 1.3.6.1.4.1.8728.2.2.2.1.2.1.2

The OID is constructed as shown in the table below:

CNIC	1.3.6.1.4.1.8728
Project Document	.2
Product Document	.2
CNIC GRID	.2
Root CA	.1
CP/CPS	.1/2
Major Version	.1
Minor Version	.2

### 1.3 Community and Applicability

CNIC GRID CA provides PKI services for the CNIC Grid research community that are involved in Grid activities.

#### 1.3.1 Organization

➤ Policy Management Authority

The decision relates to the management of CNIC GRID CA will be performed by the coordinate committee called “CNIC GRID Policy Management Authority(CNIC GRID PMA)”, which consists of representatives of Network Technology Application & Research Laboratory of CNIC. The CNIC GRID PMA will be responsible for:

- ❖ Draft and approve CP/CPS,
- ❖ Take countermeasure for compromise of the Certificate Authority(CA)'s private key,
- ❖ Take countermeasure for Emergency operations in disaster,
- ❖ Other Important matters.

➤ Operating Organization

Fig. 1-1 and Table 1-1 show organization and system configuration of the CA.

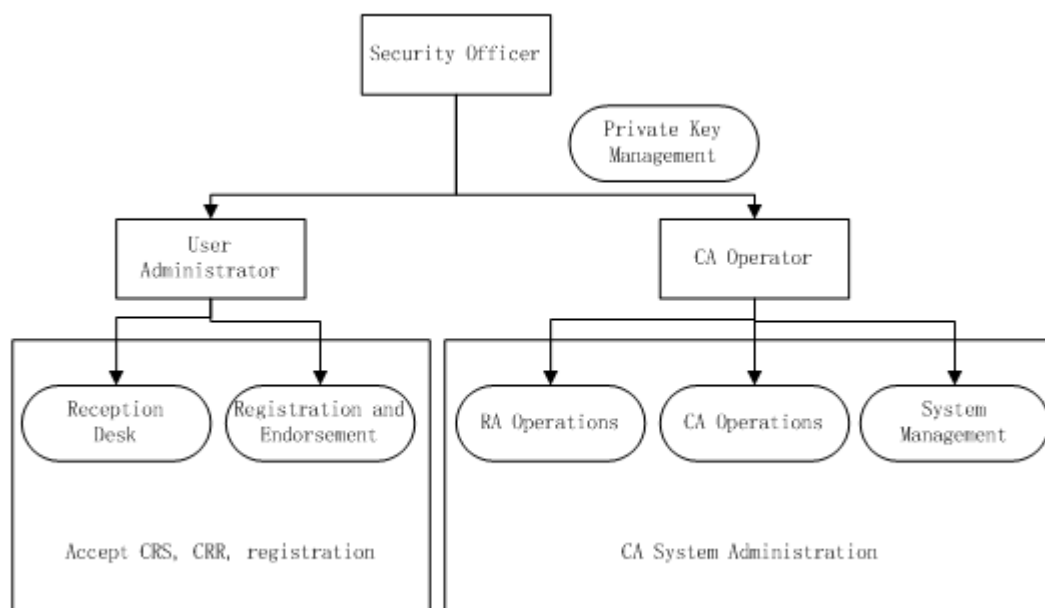


Fig 1-1 Organization and System Configuration of CNIC GRID CA

Table 1-1 Organization of operating CA and roles

Role	Main Function
Security Officer	administrates all tasks on the CA system
CA Operator	administrates RA and CA servers creates license IDs and distribute them maintains the CA system manages CA private key
User Administrator	accepts user enrollment

	examines user information and approves the user
Certificate User	a sub CA using a certificate issued by CNIC GRID CA
Host Administrator	an administrator of a host using a certificate issued by CNIC GRID CA

### 1.3.2 Certification Authorities

CNIC GRID CA only issues certificates to subordinate Certificate Authorities and system maintenance entities or servers.

### 1.3.3 Registration Authorities

CNIC GRID CA manages the functions of its Registration Authority. Additional RA's may be created as required. See the CNIC GRID CA site for a current list (<https://ca.grid.cn/ra>).

### 1.3.4 End Entities

The CNIC GRID CA issues certificates for organizations involved in the activities of CNIC Grid project or other related projects of CNIC.

### 1.3.5 Applicability

**Sub CA certificates** can be used for issuing certificates of sub CA itself. The subordinate CA certificates are used to establish PKIs.

### 1.3.6 User Restriction

The ownership of a CNIC GRID CA certificate does not imply automatic access to any kind of data resources of CNIC GRID and other sub-CAs' resources.

## 1.4 Contact Details

### 1.4.1 Specification administration organization

The CNIC GRID CA is managed by the CNIC GRID PMA.

### 1.4.2 Contact Person

The contact persons for questions related to this document or the CNIC GRID CA in general is:

**Morrise Xu**

Phone: +86 10 58812340

Address: No.4,4th South Street, Zhong Guan Cun, Haidian District,P.O.Box 349,Beijing.

Fax: +86 10 58812306

Email : gridca@cnic.cn

Web : <http://ca.grid.cn/>

## 2 General Provisions

### 2.1 Obligations

#### 2.1.1 CA Obligations

The **CNIC GRID CA** will:

- Accept certification requests from entitled entities;
- Notify the RA of certification request and accept authentication results from the RA;
- Issue certificates based on the requests from authenticated entities;
- Notify the subscriber of the issuing of the certificate;
- Publish the issued certificates (optionally, respective of privacy and other issues);
- Accept revocation requests according to the procedures outlined in this document;
- Authenticate entities requesting the revocation of a certificate, possibly by delegating this task to a CNIC GRID RA;
- Issue a Certificate Revocation List (CRL) timeliness (See section 4.4.4 and 4.4.9);
- Identify which CP/CPS is used to issue certificates;
- Publish the CRL issued; and
- Keep audit logs of the certificate issuance process (archive the certificate and certificate request).

#### 2.1.2 RA Obligations

A **CNIC GRID RA** will:

- Accept authentication requests from the CNIC GRID CA;
- Validate the certificate request;
- Authenticate entity making the certification request according to procedures outlined in this document;
- Notify the CNIC GRID CA when authentication is completed for a certification or revocation request;
- Accept revocation requests according to the procedures outlined in this document;
- Notify the CNIC GRID CA of all signing requests and revocation requests;
- Will not approve a certificate with a lifetime greater than CNIC Grid CA lifetime;
- Keep audit logs of the certificate registration process (archive the certificate request); and
- Send a Certificate Revocation Number (**CRIN-code**) which is for revoking certificate in an encrypted mail, possibly delegated this task by a CNIC GRID CA; and
- Export the CSRs and CRRs; and
- Import the certificates and CRLs.

### 2.1.3 Subscriber Obligations

Subscribers MUST:

- Read and adhere to the procedures published in this document;
- Generate a key pair using a trustworthy method;
- Take restrict precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
  - For sub CA certificates:
    - ✧ Selecting a pass phrase of a minimum recommended 15 characters;
    - ✧ Protecting the pass phrase from others;
    - ✧ Always using the pass phrase to encrypt the stored private key; and
    - ✧ Never sharing the private key with other users; and
    - ✧ Storing them encrypted whenever possible; and
    - ✧ They may be kept encrypted on the host that they represent;
- Provide correct subscriber's information and optionally authorize the publication of the certificate;
- Take restrict precautions to prevent any loss, disclosure or unauthorized use of the CRIN-code;
- Notify the CNIC GRID CA immediately in case of private key loss or compromise; and
- Use the certificates for the permitted uses only.

### 2.1.4 Relying Party Obligations

Relying parties MUST:

- Download the CA certificate and CRLs;
- Read the procedures published in this document;
- Use the certificates for the permitted uses only; and
- Do not assume any authorization attributes based solely on an entity's possession CNIC GRID CA certificate.

Relying parties should:

- Verify that the certificate is not on the CRL before validating a certificate.
- The certificate shall not be modified;
- Within validity dates;
- Checking the trust CA signature

### 2.1.5 User Administrator Obligations

User administrator will :

- Accept certified users, examine requests based on user information which is previously registered, and approve the enrollment.
- Contact the end entities and date in-person meetings or ask the official documents signed by CNIC GRID members.
- Notify the CA operators which request can be approved or deleted.

## **2.1.6 Repository Obligations**

CNIC GRID CA will provide access to CNIC GRID CA information, as outlined in section 2.6.1, on its web site, <http://ca.grid.cn>.

## **2.2 Liability**

### **2.2.1 CA liability**

The CNIC GRID CA has liability:

- To perform practices on the procedures according to the practices described in this document to validate identity. No liability, implicit or explicit, is accepted. CNIC GRID CA and its agents make no guarantee about the security or suitability of a service that is identified by a CNIC GRID certificate.
- The certification service is run with a reasonable level of security, but it is provided on a best-effort 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.
- CNIC GRID CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.
- No financial liability with respect to use or management of any issued certificate.

### **2.2.2 RA liability**

The CNIC GRID RA has a liability:

- To perform practices based on the document to protect unauthorized access or modification to confidential information contained in enrollment requests.
- Take restrict precautions to prevent any loss, disclosure or unauthorized access the subscriber's individual information.

### **2.2.3 Certificate Users and host administrators liability**

Certificate Users and host administrators have liability to protect certificates and private keys from compromised.

### **2.2.4 Relying party liability**

No stipulation

### **2.2.5 User Administrator liability**

User administrator has a liability to ensure that enrollment information to CNIC GRID CA is correct.

## **2.2.6 Repository liability**

CNIC GRID CA repository has a liability

- To response to retrieve requests within operating time defined in this document.
- Not to have a liability to ensure the CRL is the newest one available at the time of the retrieval request.

## **2.3 Financial Responsibility**

CNIC GRID CA assumes no financial responsibility with respect to the use or management of any issued certificate.

## **2.4 Interpretation and Enforcement**

This document MUST be treated according to People Republic of China(PRC) laws. Legal disputes arising from the operation of the CNIC GRID CA will be treated according to PRC laws.

### **2.4.1 Governing Law**

Interpretation of this CP and CPS is according to PRC laws.

### **2.4.2 Serverability, survival, merge, notice**

In the event that CNIC GRID CA ceases operation, all subscribers, sponsoring organizations, RAs, RSPs, and Qualified Relying Parties will be promptly notified of the termination. All certificates issued by the CNIC GRID CA that reference this Policy will be revoked no later than the time of termination.

### **2.4.3 Dispute resolution procedures**

No stipulation.

## **2.5 Fees**

No fees are charged.

## **2.6 Publication and Repositories**

### **2.6.1 Publication of CA information**

CNIC GRID CA will operate a secure online repository that contains:

- The CNIC GRID CA's certificate;

- Certificates issued by the CNIC GRID CA (optionally, respective of privacy and other issues);
- A Certificate Revocation List;
- A copy of this policy; and
- Other information deemed relevant to the CNIC GRID CA.

### **2.6.2 Frequency of Publication**

- Certificates will be published to the CNIC GRID CA repository as soon as issued (optionally, respective of privacy and other issues);
- CRLs will be published soon after a revocation is issued or refreshed once every 23 days before the 30-days validity of the CRL expires;
- All CNIC GRID CA documents will be published to the project website as they are updated; and
- Changes to this CP and CPS will be published as soon as they are approved and previous versions will remain available on-line.

### **2.6.3 Access Controls**

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.

CNIC GRID CA does not impose any access control on its policy, its signing certificate and issued certificates, nor its CRLs.

### **2.6.4 Repositories**

The repository of certificates and CRLs is available at <http://ca.grid.cn/>. The end entity certificates and CRLs MUST be signed by the CA certificate.

## ***2.7 Compliance Audit***

### **2.7.1 Frequency of Entity Compliance Audit**

The CNIC GRID CA will accept at least one external Compliance Audit per year. In addition, the CNIC GRID CA performs operational self-assessment of CA/RA staff at least once per year.

### **2.7.2 Identity/Qualifications of Auditor**

The CA will be audited by other APGrid PMA CAs.

### **2.7.3 Auditor's Relationship to Audited Party**

It is desirable that the auditor is a third-party to this PKI system.

### **2.7.4 Topics Covered by Audit**

Audit items will be selected based on the minimum CA requirements enacted by the Asia Pacific Grid Policy Management Authority. The audit **MUST** cover both compliance audit and operational audit.

### **2.7.5 Actions taken as a result of deficiency**

The CNIC GRID security group has the responsibility for the action to be taken as a result of deficiency. When the CNIC GRID CA 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.

### **2.7.6 Communication of results**

The result of the audit will be made available to members of any policy management authorities in which the CNIC GRID CA participates. It may make the results of the audit publicly available. The decision will be made by the CNIC GRID security group in case-by-case basis.

## ***2.8 Confidentiality***

### **2.8.1 Types of information to be kept confidential**

Except explicit information specified in CPS[2.6.1 publication] , all other information will be treated as confidential. Confidential information will not be provided to any other people. Confidential information including personal registration information, documents and electronic media will be stored securely by a person in charge as a security officer.

### **2.8.2 Information Considered Not Confidential**

Information specified in CPS[2.6.1 publication] is not confidential information in this system.

### **2.8.3 Disclosure of certificate revocation/suspension information**

The revocation date and reason is published when the certificate is revoked by the CA. It is not confidential information but other detailed information will not be published.

### **2.8.4 Release to law enforcement officials**

No stipulation.

### **2.8.5 Release as part of civil discovery**

No stipulation.

### **2.8.6 Disclosure upon owner's request**

Following information will be disclosed after the owner will be authenticated.

- Contents of the certificate
- Certificate status

### **2.8.7 Other information release circumstances**

No stipulation.

## ***2.9 Intellectual Property Rights***

A conforming CA MUST NOT claim any intellectual property rights on issued certificates.

# **3 Identification and Authentication**

## ***3.1 Initial Registration***

### **3.1.1 Types of names**

The subject name is an X.500 name type, a *Distinguished Name*. It has one of the following forms:

- **Sub CA**

MUST include the *full organization/project name of the sub CA* just like CN=Scientific Data Grid CA,DC=SDG,DC=Grid,DC=CN.

Note: The sub CA DN must add DC=*abbreviation of organization/project* between the CN and DC=Grid,DC=CN.

- **Person**

MUST include the *full name* of the subject just like Morrise Xu, and Email Address. For example: E=morrise@cnic.ac.cn,CN=Morrise Xu,DC=Grid,DC=CN;

➤ **Host**

MUST include the *fully qualified domain name* of the host just like sdb6800.sdg.ac.cn. For example: CN= sdb6800.sdg.ac.cn,DC=Grid,DC=CN;

### **3.1.2 Name Meanings**

The Subject Name in a certificate MUST have a reasonable association with the authenticated name of the subscriber.

### **3.1.3 Rules for Interpreting Various Name Forms**

See sections 3.1.1 and 3.1.2.

### **3.1.4 Uniqueness of Names**

The CNIC GRID CA guarantees the uniqueness of the subject names. In case of name collision when more than one entity use the same name, an uniqueness emailaddress of the end entity is appended to the DN to make the name unique.

The X.500 Distinguished Name (DN) MUST be unique for each subject name certified by the CNIC GRID CA. The Common Name (CN) component of the DN will include the full name of the subscriber as described in 3.1.1.

*Certificates MUST apply to unique individuals or resources. Users MUST not share certificates.*

The CNIC GRID CA will make reasonable attempts to ensure that a DN is not reused. If a person requests a certificate with the same DN as an existing certificate (regardless of the status of this certificate) and the request is not a renewal, the RA Operator will consult the original Personal Information to ensure that the Subscriber is the same as the person who was identified in the original certificate.

### **3.1.5 Name Claim Dispute Resolution Procedure**

No stipulation.

### **3.1.6 Recognition, Authentication, and Role of Trademarks**

No stipulation.

### **3.1.7 Method to Prove Possession of Private Key**

No stipulation.

### **3.1.8 Authentication of Organization Identity**

The CNIC GRID CA verifies the identity of organizations by checking:

- That the organization which is a grid project or community is interested in joining us as a subCA; and
- That the organization is related to CNIC.

### **3.1.9 Authentication of Individual Identity**

For certificate application, the CNIC GRID UA verifies the identity of a person by checking:

- CNIC staff will be identified by inspection employee's card.
- Users in other organizations will be identified by in person interview. Photo-id or valid official documents must be presented at the interview and UA will preserve the copy of the individual material. The Video Conference may be used for the inspection alternatively.

For certificate revocation, the RA will check the signed email, signed revocation request or CRIN-code to authenticate the user's identity. CRIN stands for a Certificate Revocation Number which will be used to revoke the certificate. Since the CRIN email is encrypted by the user's certificate, only the user can decrypt the email and get CRIN to revoke his certificate.

## **3.2 Routine Rekey**

no stipulation.

## **3.3 Rekey After Revocation**

A public key whose certificate has been revoked for private key compromise **MUST NOT** be re-certified. The public key **MAY** be re-certified if the revocation is only due to certificate expiration. In the latter case the rekey authentication **MAY** be accomplished with the same procedure indicated in Section 3.1 for initial registration or using digitally signed requests. These requests **MUST** be sent to the CA before certificate expiration.

## **3.4 Revocation Request**

The end entities **MUST** use the CRIN-code which they have received in an encrypted mail after applying a certificate successfully to generate the revocation request; or

If they do not have CRIN-code but have a certificate and a private key then they can ignore the CRIN-code and sign a digital signature with the request; or

If they have no CRIN-code and have no certificate, they need send official document to the RA (email:gridca@cnic.cn). The RA operator can revoke the certificates for the end entities.

The CNIC GRID CA checks the identity of the revoker as section 3.1.9.

Revocation request is confirmed that user and organization is authenticated by certificates issued based on this CPS.

## 4 Operational Requirements

### 4.1 Certificate Application

#### ➤ Certificate application

Users MUST generate keypair and CSR at local machines with certutility tool provided by CNIC Grid CA or OpenSSL or WinAPI. Then users need to fill the form and upload the certificate signing requests through the RA website. User administrator of the CNIC GRID RA examines the request according to this document [3.1.9 user identification]. If the application is valid, then the CNIC GRID RA approves the request and informs the CNIC GRID CA that the request has been approved. Signed email is used for the notification from the user administrator to CNIC GRID RA, or from CNIC GRID RA to the CNIC GRID CA. Then, the CNIC GRID CA will issue the request and send a plaintext mail to users with certificate serial number and certificate downloading links which will be used for obtaining a certificate from the RA server on-line. And also an email, which includes CRIN(a random passphrase generated by CA) and is encrypted with users' certificates, will be sent to the requestor. The users can decrypt the CRIN email with their private key. Detailed procedure for certificate application is described in "CNIC GRID CA User Manual" which is available on the CNIC GRID CA PKI repository.

#### ➤ Certificate enrollment

User need to create a key pair on user's local machine with 2048 bits length by using the WinAPI, OpenSSL or the CNIC GRID CA certificate utility according to the procedures described in "CNIC GRID CA Enrollment Manual", then upload a certificate signing request which contains the public key to the RA server on-line. Communication path to this enrollment is encrypted using SSL. Detailed instruction for certificate enrollment is described in "CNIC GRID CA User Manual" which is available on the CNIC GRID CA PKI repository.

### 4.2 Certificate Issuance

A certificate utility which runs on the subordinate CA server with a JVM-enabled environment is provided for users. The utility supports creation of key pairs, making CSR, or request certificate using OpenSSL.

In the case of issuing a new certificate, approved certificate requests will be signed no more than two business days, and the signed certificates will be made available online shortly afterwards. Emails will be sent to new certificate holders, if they have supplied an email address.

#### 4.2.1 Receipt Certificate Enrollment

User administrator will execute the following steps after receipt of user certificate request:

- Check the request;
- Date an in-person interview;
- Receive the official documents;
- Refuse the request if fail to authenticate the end entity identity;

- Notify the RA server about the result of checking;
- Inform the users the reason why the request could not be accept.

RA will execute the following steps after notification:

- Approve or delete the request;
- Copy the certificate signing request to the CA server using USB key.
- Notify the end entities while the certificate is successfully issued by email.

#### **4.2.2 Insurance Certificate**

CA server issues the subordinate CA certificate. RA server will notify the end entities by email with successful issuing certificate information and CRIN-code.

#### **4.2.3 Subscribe Certificate**

Users can retrieve certificates by clicking the link in the email which will be sent by RA when user certificate is successfully issued. Users also can browse the RA website and get certificates by the certificate serial number.

### ***4.3 Certificate Acceptance***

After users register user information in the RA website, UA will view the register information and decide whether the application should be approved. If it's necessary to approve the application, the register information will be register to the certificate stores(PostgreSQL Database) automatically.CA will issue the certificates and RA will enroll the certificates to the certificate stores automatically based on the user's operational document. But if it's necessary to reject the application, the UA will notify the unsuccessful candidate and will, wherever possible, inform them the reason why the application was rejected and then delete the application.

### ***4.4 Certificate Suspension and Revocation***

#### **4.4.1 Circumstances for Revocation**

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

- The subscriber's private key is lost or suspected to be compromised;
- The information in the subscriber's certificate is suspected to be inaccurate;
- The subject has failed to comply with the rules in this policy;
- The system to which the certificate has been issued has been retired;
- The subscriber no longer needs the certificate to access a relying parties' resources;
- The subscriber leaves the CNIC GRID organization; and
- The subscriber violated his/her obligations.

#### **4.4.2 Who Can Request Revocation**

The following entities can request the revocation of a certificate:

1. The entity who originally made the certificate request.
2. The entity which can prove its current responsibility for a certified machine or service.
3. The entity which can prove that he is the security officer of the sub-CA certificate.
4. The PMA of sub-CA.
5. The PMA of CNIC Grid CA.
6. The issuing CA or the associated RA.

#### **4.4.3 Procedure for Revocation Request**

A certificate revocation can be requested as outlined in section 3.4.

In case of the RA can independently confirm that the certificate has been compromised or misused, the RA notify the CA to revoke the certificate, even if the request comes from an unauthenticated source and/or the holder of the certificate is unreachable.

In case of the revocation request is signed by the owner's certificate, the RA can authenticate the request and notify the CA to revoke the certificate.

In all other cases the RA SHOULD authenticate the revocation request and try to contact the subscriber by the phone or email before revoking the certificate.

If the revoked certificate is a CA certificate the CA SHALL inform the subscribers and cross-certifying CAs in addition and SHALL terminate the certificate and CRLs distribution service for certificates/CRLs which have been issued using the compromised private key.

#### **4.4.4 Revocation Request Grace Period**

The CNIC Grid CA MUST respond within two days (excluding weekends and public holidays) to revocation requests. It SHALL however handle revocation requests with priority as soon as the request is recognized as such.

#### **4.4.5 Circumstances for Suspension**

Do not offer the suspension service.

#### **4.4.6 Who Can Request Suspension**

No stipulation.

#### **4.4.7 Procedure for Suspension Request**

No stipulation.

#### **4.4.8 Limits on Suspension Period**

No stipulation.

#### **4.4.9 CRL Issuance Frequency**

CRLs are issued after every certificate revocation or every 23 days before the 30-day validity of the CRL has expired.

#### **4.4.10 CRL Checking Requirements for Relying Parties**

A relying party may verify a certificate against the most recent CRL issued, in order to validate the use of the certificate.

#### **4.4.11 Online Revocation/Status Checking Availability**

OCSP is not implemented.

#### **4.4.12 Online Revocation Checking Requirements**

No stipulation.

#### **4.4.13 Other Forms of Revocation Advertisement Available**

No stipulation.

### ***4.5 Security Audit Procedures***

The CNIC GRID CA will retain records as much as possible so that the CNIC GRID CA could trace anything if something illegal would happen. Such audit information is not publicly available. Auditors are allowed to access to the information as part of auditing and such information must be kept confidential.

#### **4.5.1 Types of event recorded**

- CA system logs
  - ✧ Access and operation logs to the CA daemon process
  - ✧ Error logs for accesses and operations to the CA daemon process
  - ✧ Operation logs of the CA daemon process
- RA system logs
  - ✧ Access and operation logs to the RA daemon process
  - ✧ Error logs for accesses and operations to the RA daemon process

- Linux system logs
  - ✧ shutdown/boot/reboot logs of the CA server and the RA server
  - ✧ login/logout/sudo logs of the CA and the RA server
  - ✧ other logs archived by Linux operation of the CA and the RA server
  - ✧ secure/cronlog/maillog/messages(sulog)syslog/errorlog
- Logs of physical access to the CA machines
  - ✧ Paper sheets which record all events about the access to the CA machines. The events include the names of CA operators, date and time of entering/leaving the CA room, and the purpose of the access to the machines.
  - ✧ Access logs to the CA machines those are recorded by the Security Officers of CNIC GRID CA.

Archive information will be verified using the event records of accesses to the CA machines.

#### **4.5.2 Frequency of processing log**

No stipulation

#### **4.5.3 Retention period for audit log**

The minimum retention period is three years.

#### **4.5.4 Protection of audit log**

Access logs and System logs are protected by the authorization mechanism provided by Unix operating system. Only the owners of such logs are able to modify the logs. Access logs and System logs are periodically back-up to the offline media which is stored in a safe box. For logs of physical access to the CA machines, each paper sheet is signed by the User Administrator and is assigned a unique serial number. Filled paper sheets and access logs to the CA machines are stored in a safe box.

#### **4.5.5 Audit log backup procedures**

The electronic part of the archive is done by daily tape backup. The paper-based verification trail is stored in a safe box at CNIC.

#### **4.5.6 Audit collection system (internal vs external)**

No stipulation

#### **4.5.7 Notification to event-causing subject**

No stipulation

## 4.5.8 Vulnerability assessments

No stipulation

## 4.6 Records Archival

### 4.6.1 Types of Event Audited

- CA system logs
  - ✧ Access and operation logs to the CA daemon process
  - ✧ Error logs for accesses and operations to the CA daemon process
  - ✧ Operation logs of the CA daemon process
- RA system logs
  - ✧ Access and operation logs to the RA daemon process
  - ✧ Error logs for accesses and operations to the RA daemon process
  - ✧ Logs of issued certificates
  - ✧ All issued CRLs
  - ✧ The date of issuance of CRLs
  - ✧ All CSRs and CRRs
- Linux system logs
  - ✧ shutdown/boot/reboot logs of the CA server and the RA server
  - ✧ login/logout/sudo logs of the CA and the RA server
  - ✧ other logs archived by Linux operation of the CA and the RA server
    - ✓ secure/cronlog/maillog/messages(sulog)syslog/errorlog
- Logs of physical access to the CA machines
  - ✧ Paper sheets which record all events about the access to the CA machines. The events include the names of CA operators, date and time of entering/leaving the CA room, and the purpose of the access to the machines.
  - ✧ Access logs to the CA machines those are recorded by the Security Officers of CNIC GRID CA.
- Emails
  - ✧ All emails received by the CNIC GRID RA
  - ✧ All emails received by the user administrator
  - ✧ All emails of system-logs sent from the CA and the RA servers
- Other documents
  - ✧ A list of email addresses of end entities
  - ✧ All issued certificates
  - ✧ for each approved request, how the request was approved
  - ✧ for each rejected request, how the request was rejected
  - ✧ official documents if they are used for identification of entities
  - ✧ All versions of the CP/CPS
  - ✧ All versions of the Certificate and CRL Profile

- ✧ Internal documents for the operation of CNIC GRID CA PKI Service
- ✧ All Audit reports

#### **4.6.2 Retention Period for Audit Logs**

The minimum retention period is three years.

#### **4.6.3 Protection of Archive**

System logs and Email archives are protected by the authorization mechanism provided by Linux operating system. Only the owners of the operating system are able to modify the logs. System logs and Email archives are periodically back-up or back-up after operation to the removable media which is stored in a safe box.

For logs of physical access to the CA machines, each paper sheet is signed by the Security Officer and is assigned a unique serial number. Filled paper sheets and access logs to the CA machines are stored in a safe box.

Records for identifying requests and official documents are stored in a safe box.

#### **4.6.4 Archive Backup Procedures**

See section 4.6.3.

#### **4.6.5 Time-Stamping Requirements**

No stipulation.

#### **4.6.6 Archive Collection System**

See section 4.6.3.

#### **4.6.7 Procedures to Obtain and Verify Archive Information**

No stipulation.

### ***4.7 Key Changeover***

The CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA key should be generated one year before the old one becomes invalid. From that point on new certificates are signed by the new CA key.

The new CA public key is posted online at <https://ca.grid.cn/pub>.

### ***4.8 Compromise and Disaster Recovery***

If the CA's private key is compromised - or suspected to be compromised - the CA will:

- Inform subscribers and other relying parties;
- Terminate the issuance and distribution of certificates and CRLs;
- Generate a new CA certificate (with a new key pair) and make it immediately available in the public repository at <http://ca.grid.cn/>; and
- All subjects will have to recertify following the procedures in section 3.1.

## **4.9 CA Termination**

Termination of a CA is regarded as the situation where all services associated with a logical CA are terminated permanently.

Before the CNIC GRID CA terminates its services, it **MUST**:

- inform all subscribers, cross certifying CAs, lower level CAs and relying parties with which the CA has agreements or other form of established relations;
- make widely available information of its termination; and
- stop issuing certificates and CRLs.

A subordinate CA **MAY** terminate or continue operation as a self-standing CA.

# **5 Physical, Procedural and Personnel Security**

## **Controls**

### **5.1 Physical Security Controls**

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

#### **5.1.1 Site Location**

The CNIC GRID CA is located at the Computer Network Information Center of CAS (CNIC).

#### **5.1.2 Physical Access**

The CNIC GRID CA machines are kept in the CNIC machine room, which is locked by an finger pass lock and physical access to the room is restricted to explicitly authorized person given by CNIC. Physical access to the CA machines is restricted to CA operators given by CNIC GRID Security Officers. A CA operator is not allowed to access the CA machines alone and need to enter the room with the other CA operator. If a CA operator needs to access the machines alone, he **MUST** notify the fact to the user administrator by signed Emails before and after entering the room.

All events about the access to the room **MUST** be recorded in the paper sheets prepared by security officers. The events include the names of CA operators, date and time of entering/leaving the room, and the purpose of the access to the room. The filled sheets will be kept in a safe box.

### **5.1.3 Power and Air Conditioning**

The building has an centre air conditioning system and the CNIC GRID CA machines are connected to a UPS system.

### **5.1.4 Water Exposure**

The hardware is in a zone not subject to floods.

### **5.1.5 Fire Prevention and Protection**

The building has a fire alarm system.

### **5.1.6 Media Storage**

Backups are stored on removable storage media. Media will be stored in the lock-up box in the room where restrictly access control is done.

### **5.1.7 Waste Disposal**

No stipulation.

### **5.1.8 Off-site Backup**

No stipulation.

## ***5.2 Procedural Controls***

### **5.2.1 Trusted roles**

CA System Administrators(SA) have full control over the CA Server and software, but not over the cryptographic relevant information like the private key of the CA.

Certificate authority operators(CAO) can manage all certificates, requests, profiles and a subset of certificate authorities described by the operator access rules.

Operation System Administrators(OSA) have full control of the running and network environment of CA and RA.

Auditors have read-only access to all components of the CNIC GRID CA to verify the operation complies with the rules and regulations of this CP/CPS.

Registration authority operators(RAO) can manage a subset of certificates and requests described by the RA policies and the operator access rules.

## **5.2.2 Number of persons required per task**

The operation of this CA and its subsidiaries requires at least:

- Two SA due to the high availability requirements,
- Three CAO due to the high availability requirements and to implement dual controls for the access to the cryptographic secrets,
- Two OSA due to the high availability requirements,
- One RAO due to the high availability requirements.

## **5.2.3 Identification and authentication for each role**

Identification and authentication for all roles is archived using username and password.

## **5.2.4 Roles requiring separation of duties**

An SA may not be an CAO, OSA, or auditor.

CAO may not configure the CA or be an SA.

OSA may not be an SA, CAO or auditor.

Auditor may not be an SA, CAO, or OSA.

RAO may not be an SA, CAO, or OSA.

## **5.3 Personnel Security Controls**

Access to servers and applications is limited to the CNIC GRID CA Security Group who are staff or guest workers of CNIC. No other personnel is authorized to access CNIC GRID CA facilities without the physical presence of CA personnel.

# **6 Technical Security Controls**

## **6.1 Key Pair Generation and Installation**

### **6.1.1 Key Pair Generation**

Key pairs for the CNIC GRID CA are generated by the CNIC GRID CA Security Officers on a dedicated machine, not connected to any kind of network. The underlying software package used is OpenSSL. The algorithm used is SHA1.

Each end entity **MUST** generate its own key pair. The CNIC GRID CA does not generate end entity private keys.

### **6.1.2 Private Key Delivery to Entity**

The CNIC GRID CA never has access to the end entity private key.

### **6.1.3 Public Key Delivery to Certificate Issuer**

End entities' public keys MUST be delivered to the CNIC GRID CA as section 3.1.

### **6.1.4 CA Public Key Delivery to Users**

The CA certificate is available from its public repository at <http://ca.grid.cn>.

### **6.1.5 Key Sizes**

Keys of length less than 1024 bits will not be signed. The sub-CA's key pair length is 2048 bits.

### **6.1.6 Public Key Parameters Generation**

No stipulation.

### **6.1.7 Parameter Quality Checking**

No stipulation.

### **6.1.8 Hardware/Software Key Generation**

Key generation is performed by software (for example, OpenSSL).

### **6.1.9 Key Usage Purposes**

CNIC GRID certificates may be used only for authentication and signing proxy certificates [PROXY]. It is understood that they could be used in other capacities, but the CNIC GRID CA does not recommend or warrant any other use of the certificates it signs.

The CNIC GRID CA root private key will only be used to sign CRLs and end entity certificates.

## ***6.2 Private Key Protection***

### **6.2.1 Private Key (n out of m) Multi-person Control**

This CA and its subsidiaries do not yet support private key(n out of m) multi-person control. But the CNIC GRID CA implements multi-person control for the access to the CA server as described in this document. The passphrase encrypting the CA private key is kept by all CA operators(3 persons). No other person know the passphrase.

## **6.2.2 Private Key Escrow**

No stipulation.

## **6.2.3 Private Key Archival and Backup**

The CNIC GRID CA root private key is kept encrypted in removable devices and the removable devices are protected in a safebox.

## **6.3 Other Aspects of Key Pair Management**

The current CNIC GRID CA root certificate has a validity of twenty years, and has a key length of 2048.

The lifetime of CA certificate MUST be no less than two times of the maximum lifetime of an end entity certificate except Sub-CA certificate. The lifetime of an end entity certificate MUST be no more than CA certificate. The lifetime of Sub-CA certificate is five years to ten years according to the end entity requirements and the CNIC Grid CA's validity.

## **6.4 Activation Data**

CNIC GRID CA root private key is protected by a passphrase of a minimum recommended 15 characters.

## **6.5 Computer Security Controls**

### **6.5.1 Specific Computer Security Technical Requirements**

CNIC GRID CA servers include the following:

- Operating systems are maintained at a high level of security by applying all recommended and applicable security patches;
- Monitoring is done to detect unauthorized software changes; and
- Services are reduced to a minimum.

### **6.5.2 Computer Security Rating**

No stipulation.

## **6.6 Life-Cycle Security Controls**

No stipulation.

## **6.7 Network Security Controls**

The RA server will be online and CA server offline. The RA server is protected by the firewall. The dataexchange between RA and CA is operated manually by security way (All operations accomplish in the dedicated CA room).

## **6.8 Cryptographic Module Engineering Controls**

No stipulation.

## **7 Certificate and CRL Profiles**

### **7.1 Certificate Profile**

Certificate profile is described in a separate document, "CNIC GRID CA Certificate and CRL Profile version 1.0". The document is available on the CNIC GRID CA PKI repository.

### **7.2 CRL Profile**

CRL profile is described in a separate document, "CNIC GRID CA Certificate and CRL Profile version 1.0". The document is available on the CNIC GRID CA PKI repository.

## **8 Specification Administration**

### **8.1 Specification Change Procedures**

The CNIC GRID PMA will change this document by necessity. Revision is made and approved by the CNIC GRID PMA. Minor editorial changes to this document can be made without approval by the CNIC GRID PMA. New OID will not be assigned to the revised document when such minor changes would be made. Substantial changes in policy or changes in the technical security controls need to be approved by the CNIC GRID PMA. NEW OID will be assigned to the revised document for such substantial changes would be made.

### **8.2 Publication and Notification Procedures**

For minor editorial changes, revision to this document will be announced on the CNIC GRID CA repository. Substantial changes will be notified by Emails to all relevant relying parties, all cross-certifying CAs, and the PMAs in which the CNIC GRID CA participates. These changes will also be announced on the CNIC GRID CA repository.

### **8.3 CPS Approval Procedures**

The CNIC GRID PMA is responsible for the CP and CPS. All major changes MUST be approved by the PMA. Changes logs are described in Appendix A of this document. Whenever there is a change in the CP/CPS the O.I.D of the document must change and the major changes must be announced to the APGrid PMA and approved before signing any certificates under the new CP/CPS.

## **Glossary**

### **Activation Data**

Data values, other than keys, that are required to operate cryptographic modules and that need 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, which is digitally signed with the private key of the CA that issued it

### **Certificate Policy (CP)**

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

### **Certification Practice Statement (CPS)**

A statement of the practices, which a certification authority 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., person, host, and service 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.

### **Person Certificate**

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

### **Policy Management Authority (PMA)**

For the CNIC GRID CA this is a committee composed of the CNIC GRID CA Security Group.

### **Policy Qualifier**

The policy-dependent information that 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.

**Service Certificate**

A certificate for a particular service running on a host. It will represent a single service on a single host.

**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.

**Virtual Organization (VO)**

An organization that has been created to represent a particular research or development effort independent of the physical sites at which the scientist or engineers work.

**User Administrator(UA)**

The operator of the CA system which manages the user registrations, in-person interview, official documents and correctness individual information.

## **Bibliography**

**[CERN]**

CERN CA Certificate Policy and Certification Practice Statement, Version 0.1.  
August 2001.

**[CNRS]**

Certificate Policy and Certification Practice Statement CNRS/CNRSProjets/  
Datagrid-fr, Version 0.3. August 2002.

**[DOE]**

DOE Science Grid PKI Certificate Policy and Certification Practice Statement,  
Version 2.1. August 2002.

**[FZKGRID]**

FZK-Grid-CA Certificate Policy and Certification Practice Statement, Version 0.2.  
June 2002.

**[GRIDEIRE]**

Grid-Ireland Certification Authority Certificate Policy and Certification Practice  
Statement, Version 0.3. October 2001.

**[INFN]**

INFN CA Certificate Policy and Certification Practice Statement, Version 1.0.  
December 2001.

**[PROXY]**

S. Tuecke, et al., Internet X.509 Public Key Infrastructure Proxy Certificate  
Profile, Internet Draft. 2001.

**[AIST Grid]**

AIST GRID PKI Service Certificate Policy and Certificate Practice Statements  
Ver.1.1.1,CP OID 1.3.6.1.4.1.18936.1.11.2 and CPS OID 1.3.6.1.4.1.18936.1.11.1.1,  
June 15,2005

**[RFC2527]**

S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and

## Appendix A. Change Logs

- Version 1.0
  - Major Change
    - ✧ First Version of CNIC GRID CA
  - Minor Change
- Version 1.1
  - Major Change
    - ✧ In section 4.9, modified the procedure.
    - ✧ In section 3.3, added the detail of the Rekey after revocation.
    - ✧ In section 4.4.2, added the detail of who can request revocation.
    - ✧ In section 4.4.3, added the detail of Procedure for Revocation Request.
    - ✧ In section 4.4.4, added the detail of Revocation Request Grace Period.
    - ✧ In section 3.1.4, added the description about the uniqueness of DN.
    - ✧ In section 4.1 & 4.2, added the description of the certificate renewal procedure.
  - Minor Change
    - ✧ In section 3.1.1, modified the detail of Types of names.
- Version 1.2
  - Major Change
    - ✧ In section 1.3.2, corrected the mistakes.
    - ✧ In section 2.8, changed the description of confidential.
    - ✧ In section 4.5, added the description about security audit.
  - Minor Change
    - ✧ In section 3.1.1, modified the sub CA name.
    - ✧ In section 3.1.4, added the description of uniqueness of name.
    - ✧ In section 2.1.3, added the description of host and person certificate.
    - ✧ In section 2.1.1, added the description of CA obligation.
    - ✧ In section 3.1.9, modified the authentication of individual identity.
    - ✧ In section 4.1, modified some mistakes.
    - ✧ In section 6.1.1, deleted the basic certificate.
    - ✧ In section 2.1.3, modified the unencrypted to encrypted and rasonalbe to restrict.
    - ✧ In section 3.3, modified the suspension to expiration.
    - ✧ In section 4.1, modified the system email to signed email and added other description.
    - ✧ In section 4.2, completed the second sentence.
    - ✧ In section 4.2.2, added the delivering end entities certificate issued information.
    - ✧ In section 4.4.2, added description.
    - ✧ In section 4.4.3, modified some mistakes.
    - ✧ In section 2.1.4, added download CA certificate and CRLs and other descriptions.
    - ✧ In section 2.2.2, added the description about finacial liability.

- ✧ In section 2.2.6, corrected the description.
- ✧ In section 2.8.2, changed the title to Information Considered Not Confidential.
- ✧ In section 3.1.9, deleted the third bullet.
- ✧ In section 4.2.2, changed the description.
- ✧ In section 2.6.2 and 4.4.9, changed the description of CRL.
- ✧ In section 1.3.4, added more details.
- ✧ In section 4.2.1, added the refusing situation.
- ✧ In section 4.1, changed some description.
- ✧ In section 8.3, added some description about CP/CPS document.
- ✧ In section 4.3, changed the description about certificate acceptance.
- ✧ In section 1.1, added more description about type of certificates.