SDG CA
Certificate Policy
And
Certification Practice Statement
Version 1.2

DN: CN=SDG-CA,O=SDG,C=CN

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

Oct 14, 2005

Version History

Version	Author	Participator	Date	Comment
1.0	Morrise Xu	Kai Nan	2004-9-10	Initial Document
1.1	Morrise Xu	Kai Nan	2004-12-1	Experimental CA
1.2	Morrise Xu	Kai Nan	2005-10-14	Production CA
1.2.1	Morrise Xu	APGrid PMA members	2005-11-15	Reviewed by the APGrid PMA

Index

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 SDG for the operations of the SDG Root CA service.
Now SDG CA has only one Root CA, has no sub 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 Scientific Data Grid Certificate Authority (SDG CA), the top level CA for all purposes of *Scientific Data Grid*.

1.2 Identification

Document Title
SDG CA Certificate Policy and Certification Practice Statement
Document Version **1.2**
Document Date **Sep 10, 2004**
Last Update Date **Oct 14, 2005**
CP OID: 1.3.6.1.4.1.8728.2.2.1.8.9.1.1.2
CPS OID: 1.3.6.1.4.1.8728.2.2.1.8.9.2.1.2
The OID is constructed as shown in the table below:

CNIC	1.3.6.1.4.1.8728
Project Document	.2
Product Document	.2
SDG	.1
CA	.8
Document Serial	.9
CP/CPS	.1/2
Major Version	.1
Minor Version	.2

1.3 Community and Applicability

SDG CA provides PKI services for the Scientific Data Grid research community that are involved in Grid activities.

1.3.1 Certification Authorities

SDG CA does not issue certificates to subordinate Certificate Authorities.

1.3.2 Registration Authorities

SDG CA manages the functions of its Registration Authority. Additional RA’s may be created as required. See the SDG CA site for a current list (https://ca.sdg.ac.cn/ra).

1.3.3 End Entities

The SDG CA issues certificates for people, hosts, and host applications involved in the activities listed in section 1.3.

1.3.4 Applicability

Person certificates can be used to authenticate a person to research sites that have agreed to accept certificates from the SDG CA, and may require the signing of Globus proxy certificates [PROXY]. While person certificates can be used for other purposes such as email signing, etc.
Service certificates can be used to identify a named service on a specific host and for encryption of communication (SSL/TLS).

1.3.5 User Restriction

The ownership of a SDG certificate does not imply automatic access to any kind of data resources of SDG.

1.4 Contact Details

1.4.1 Specification administration organization

The SDG CA is managed by the Scientific Data Grid Security Group.

1.4.2 Contact Person

The contact persons for questions related to this document or the SDG 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 : sdgca@cnic.cn
Web : https://ca.sdg.ac.cn/pub

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

The **SDG 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 SDG RA;
- Issue a Certificate Revocation List (CRL);
- 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 **SDG RA** will:

- Accept authentication requests from the SDG CA;
- Validate the certificate request;
- Authenticate entity making the certification request according to procedures outlined in this document;
- Notify the SDG CA when authentication is completed for a certification or revocation request;
- Accept revocation requests according to the procedures outlined in this document;
- Notify the SDG CA of all revocation requests;
- Will not approve a certificate with a lifetime greater than 12 months;
- Keep audit logs of the certificate registration process (archive the certificate request); and
- Send CRIN-code for revocating certificate with an encrypted mail, possibly by delegating this task to a SDG CA;

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 reasonable precautions to prevent any loss, disclosure or unauthorized use of the

private key associated with the certificate, including:

- ✧ For Person Certificates:
- ✧ Selecting a pass phrase of a minimum recommended 12 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;
- ✧ For Service Certificates:
- ✧ Storing them encrypted whenever possible; and
- ✧ They may be kept unencrypted on the host that they represent;

- ➢ . Provide correct personal information and optionally authorize the publication of the certificate;
- ➢ Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the CRIN-code;
- ➢ . Notify the SDG 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:

- ➢ . 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 SDG CA certificate.

Relying parties should:

- ➢ Verify that the certificate is not on the CRL before validating a certificate.

2.1.5 Repository Obligations

SDG CA will provide access to SDG CA information, as outlined in section 2.6.1, on its web site, https://ca.sdg.ac.cn/pub.

2.2 Liability

2.2.1 CA liability

The SDG 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.SDG CA and its agents make no guarantee about the security or suitability of a service that is identified by a SDG 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.

- SDG CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

2.2.2 RA liability

The SDG RA has a liability:

- To perform practices based on the document to protect unauthorized access or modification to confidential information contained in enrollment requests.

2.2.3 Certificate Users and host administrators liability

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

2.3 Financial Responsibility

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

2.4 Interpretation and Enforcement

This document must be treated according to Pepole Republic of China(PRC) laws. Legal disputes arising from
the operation of the SDG 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, survial, merge, notice

In the event that SDG CA ceases operation, all subsribers, sponsoring organizations, RAs, RSPs, and Qualitified Relying Parties will be promptly notified of the termination.
All certificates issued by the SDG 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

SDG CA will operate a secure online repository that contains:

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

2.6.2 Frequency of Publication

- Certificates will be published to the SDG CA repository as soon after being issued (optionally, respective of privacy and other issues);
- CRLs will be published soon after a revocation is issued or refreshed once every 30 days, 7 days before the month-long validity of the CRL expires;
- All SDG 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.
SDG CA does not impose any access control on its policy, its signing certificate and issued certificates, and its CRLs.

2.6.4 Repositories

The repository of certificates and CRLs are available at https://ca.sdg.ac.cn/pub. 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 SDG CA will accept at least one external Compliance Audit per year. In addition, the SDG 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 SDG security group has the responsibility for the action to be taken as a result of deficiency. When the SDG 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 SDG CA participates. It may make the results of the audit publicly available. The decision will be made by the SDG security group in case-by-case basis.

2.8 Confidentiality

SDG CA collects subscribers' 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 generally not considered confidential. The SDG CA does not collect any other kind of confidential information.The SDG CA does not have access to or generate the private keys of a digital signature key pair, such as those used in SDG identity certificates. These key pairs are generated and managed by the client and are the sole responsibility of the subscriber.

2.9 Intellectual Property Rights

Parts of this document are inspired by [SDG CA], and [RFC2527].

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:

- **Person**

Must include the *organization name* and *full name* of the subject just like CNIC-morrise, comprising organization name and full name;

- **Host**

Must include the *fully qualified domain name* of the host just like leo.sdg.ac.cn, comprising organization name and domain name;

- **Service**

Must include the *organization name , fully qualified domain name* and *named service* just like CNIC-leoCHH, comprising organization name and named service.

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

For hosts and services the CN should contain the fully qualified domain name (FQDN) of the host.

The CN may contain an arbitrary alphanumeric qualifier that distinguishes it from certificates from the same subscriber .

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

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 SDG CA verifies the identity of organizations by checking:

- That the organization is known to be part of a SDG project or related experiments; and
- That the organization is operating in CAS, by checking contact information.

3.1.9 Authentication of Individual Identity

The SDG RA verifies the identity of a person by checking:

- A request must be generate by the site https://ca.sdg.ac.cn/pub; and
- The individual information must be sent to sdgca@cnic.cn with an email subject containing “Certificate Request” (or “Certificate Revocation”) and originate from a valid email address from a known organization as specified in section 3.1.8; and
- A request will be accepted if the person is known to those listed in section 1.4; or
- A request is verified by an RA closely associated with the person’s organization; or
- A request is verified by his information and photo identify sent by a person; or
- The revocation request must be sent via a secure method such as signed email; or
- A revocation request generated by the website with user’s signature or CRIN code.

3.2 Routine Rekey

no stipulation.

3.3 Rekey After Revocation

no stipulation.

3.4 Revocation Request

The end entities must use the CRIN-code to generate the revocation request which they received in an encrypted mail after applying a certificate successfully; 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:sdgca@cnic.cn). The RA operator can do this.

The SDG CA checks the identity of the revoker as section 3.1.9.

4 Operational Requirements

4.1 Certificate Application

The minimum key length for all certificates is 1024 bits. The maximum validity period is one year. Each applicant must generate its own key pair using either Globus or OpenSSL or similar software.
Certificate requests in PEM format are sent by the server certificate application, as outlined in section 3.1.9.

4.2 Certificate Issuance

SDG CA issues the certificate if, and only if, the authentication of the subject is successful according to section 3.1.9. The applicant will be notified about the issuance of the certificate by email or will be informed about the reason why the certificate could not be issued.

4.3 Certificate Acceptance

No stipulation.

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 SDG organization; and
- The subscriber violated his/her obligations.

4.4.2 Who Can Request Revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of a circumstance of revocation or by the SDG RA.

4.4.3 Procedure for Revocation Request

A certificate revocation can be requested as outlined in section 3.1.9.

4.4.4 Revocation Request Grace Period

There is no revocation grace period.

4.4.5 Circumstances for Suspension

No stipulation.

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 30 days, 7 days before the 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

Security auditing of the SDG CA is not supported.

4.6 Records Archival

4.6.1 Types of Event Audited

The following events are recorded and archived:

- Certificate requests;
- Certificate revocation requests;
- Issued certificates;
- Issued CRLs; and
- All email correspondence with the SDG CA; and
- login/logout/reboot of the machine.

4.6.2 Retention Period for Audit Logs

The minimum retention period is three years.

4.6.3 Protection of Archive

Records are backed up on removable media, which are stored in a room with restricted access.

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.sdg.ac.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 https://caadm.sdg.ac.cn/ca/; and
- All subjects will have to recertify following the procedures in section 3.1.

4.9 CA Termination

Before the SDG CA terminates its services, it will:

- Inform subscribers and subordinate RAs;
- Make widely available information of its termination; and
- Stop issuing certificates and CRLs.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

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

5.1.1 Site Location

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

5.1.2 Physical Access

Physical access to the hardware is restricted to authorized personnel of SDG Security Group. All removable media is stored in secured area.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the SDG 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, request, 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 enviroment of CA and RA.
Auditors have read-only access to all components of the SDG 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 it subsidiaries requires at least:

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

5.2.3 Identification and authentication for each role

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

5.2.4 Roles requiring seperation 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 SDG CA Security Group who are staff or guest workers of CNIC. No other personnel is authorized to acces SDG 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 SDG CA are generated by the SDG CA Security Group on a dedicated machine, not connected to any kind of network. The underlying software package used is OpenSSL.
Each end entity must generate its own key pair. The SDG CA does not generate end entity private keys except basic certificate.

6.1.2 Private Key Delivery to Entity

The SDG 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 SDG CA as section 3.1.

6.1.4 CA Public Key Delivery to Users

The CA certificate is available from its public repository at https://ca.sdg.ac.cn/pub.

6.1.5 Key Sizes

Keys of length less then 1024 bits will not be signed.

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

SDG 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 SDG CA does not recommend or warrant any other use of the certificates it signs.
The SDG 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) muti-person control.

6.2.2 Private Key Escrow

No stipulation.

6.2.3 Private Key Archival and Backup

The SDG CA root private key is kept encrypted in removable devices.

6.3 Other Aspects of Key Pair Management

The current SDG CA root certificate has a validity of five years, expires in 2009-11-17, and has a key length of 2048.

According the discussions on lifetime of CA certificate, our next SDG CA root certificate will have a validity of ten years.

The lifetime of CA certificate must be no less than two times of the maximum lifetime of an end entity certificate.

6.4 Activation Data

SDG 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

SDG 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

7.1.1 Version Number

X.509 v3.

7.1.2 Certificate extensions

Basic Constraints (CRITICAL):Not a CA（Only for the end entity certificate）
Key Usage (CRITICAL):

- End entity certificate
  - Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
- CA certficate
  - Digital Signature, Non Repudiation, Key Encipherment

Subject Key Identifier: Used for all certificates
Authority Key Identifier: Used for all certificates
Subject Alternative Name: Subject's email address
Issuer Alternative Name: none

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer
C=CN, O=SDG, CN=SDG-CA
Person
C=CN, O=SDG, OU=*Certficate request group*, CN= *organizationName-fullPersonName*
Hosts
C=CN, O=SDG, OU= *Certficate request group*, CN= *hostName*
Service
C=CN, O=SDG, OU= *Certficate request group*, CN= *organizationName-serviceName*

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints Extensions

No stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

No stipulation.

7.2 CRL Profile

7.2.1 Version

X.509 v3.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8 Specification Administration

8.1 Specification Change Procedures

Users may not be warned in advance of changes to SDG CA's policy and CPS. Relevant changes will be made as widely available as possible.Whenever there is a change in the CP/CPS, the O.I.D. of the document must change.

8.2 Publication and Notification Procedures

The policy is available at https://ca.sdg.ac.cn/pub, and the major changes must be announced to the APGrid PMA.

8.3 CPS Approval Procedures

The SDG CA Security Group is responsible for the CP and CPS. All changes must be approved by the APGrid PMA.

Glossary

Act ivat ion 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 SDG CA this is a committee composed of the SDG 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.

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.

[RFC2527]

S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527. March 1999.