Academia Sinica Grid Computing Certification Authority (ASGCCA) Certificate Policy and Certification Practice Statement

version 1.1

June 2003

Contents

1 Introduction

1.1 Overview

This is a document based on the structure suggested by the “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” [RFC 2527]. Sections that are not included have a default value of "No stipulation". This document describes the set of rules and procedures established by the Academia Sinica Grid Computing Certification Authority (ASGCCA), the Certification Authority for the Academia Sinica Grid Computing Service.
(http://grid.sinica.edu.tw).

1.1.1 General Definitions

The document makes use of the following terms.

- Academia Sinica Grid Computing Directory Service (ASGCDS)

  Academia Sinica Grid Computing Directory Service keeps the user’s information. For example, name, e-mail, phone numbers, office, institute, work groups, working projects, who is the superior, etc. The information is not published.

- 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 pass phrase, or a manually-held key share).

- ASGCCA

  The abbreviation of Academia Sinica Grid Computing Certification Authority.

- 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.

- Issuing certification authority (issuing CA)

  In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

- 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.

- Set of provisions

  A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.

1.2 Identification

- Document title:

  Academia Sinica Grid Computing Certification Authority (ASGCCA) Certificate Policy and Certification Practice Statement

- Document version:

  1.1

- OID:

  The following ASN.1 Object Identifier (OID) has been assigned to this document: 1.3.6.1.4.1.5935.10.1.1.1. This OID is constructed as shown in the table below

IANA	1.3.6.1.4.1
Academia Sinica Computing Centre	.5935
ASGCCA	.10
CP/CPS	.1
Major Version	.1
Minor Version	.1

- Document date:
  June 2003

1.3 Community and Applicability

1.3.1 Certification Authorities

ASGCCA is managed by Acdemia Sinica Computing Centre.

1.3.2 Registration Authorities

Academia Sinica Computing Centre manages the functions of the ASGCCA Registration Authority under the rule of this CP-CPS.

1.3.3 End Entities

ASGCCA issues certificates for the following subjects:

- Users of Academia Sinica Computing Centre
- Users of Domestic/International Grid-based Application/Projects.

1.3.4 Applicability

The certificates issued by ASGCCA must not be used for financial transaction.
The authorised uses of certificate issued by ASGCCA are:

- e-mail signing and encryption (S/MIME)
- authentication and encryption of communication (SSL/TLS)
- object-signing

1.4 Contact Details

The ASGCCA is managed by Academia Sinica Computing Centre (http://www.ascc.net).
Contact person for questions related to this document or the ASGCCA in general:

Yuan, Tein Horng
Mail Box: Nankang PO BOX 1-8 Taipei, Taiwan 11529
Address: 128, Sec. 2, Academia Road, Nankang, Taipei, Taiwan 11529
Phone: +886-2-2789-9247
Mobile: +886-921-931977
Fax: +886-2-2783-6444
email: asgcca@grid.sinica.edu.tw

2 General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

- Accept certificate signing request from acceptable entities (see section 1.3.3);
- Authenticate entities according to procedures outlined in this document;
- Issue certificates based on the requests from authenticated entities;
- Notify the subscriber about the certificate issuance;
- Publish the issued certificates;
- Accept certificate revocation requests from entities;
- Authenticate entities requesting the revocation of certificate;
- Issue CRLs according with the rules described in this document;
- Publish the issued CRLs;
- Follow the policies and procedures described in this document.

2.1.2 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:
  - Selecting a pass phrase of at minimum 8 characters
  - Protecting the pass phrase from others
- Provide correct personal information and authorize the publication of the certificate.
- Notify immediately ASGCCA in case of private key loss or compromise.
- User must not share certificate.

2.1.3 Relying Party Obligations

Relying parties must:

- Read the procedures published in this document.
- Verify the certificate by checking whether the validity period has expired and whether the certificate is on the latest CRL.
- Use the certificates for the permitted uses only.

2.1.4 Repository Obligations

ASGCCA will publish certificates and CRLs as soon as issued.

2.2 Liability

ASGCCA only guarantees to control the identity of the subjects requesting a certificate according to the practices described in this document. No other liability, implicit or explicit, is accepted.

ASGCCA will not give any guarantees about the security or suitability of the service that is identified by a ASGCCA 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.

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

2.3 Financial Responsibility

No Financial responsibility is accepted.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Interpretation of this policy is according to R.O.C. laws.

2.5 Fees

No fees are charged for ASGCCA Certificates.

2.6 Publication and Repositories

2.6.1 Publication of CA information

ASGCCA will operate a secure online repository that contains:

- ASGCCA's certificate;
- Certificates issued by ASGCCA;
- A Certificate Revocation List;
- A copy of this policy;
- Other information relevant to the ASGCCA.

2.6.2 Frequency of Publication

1. Certificates will be published as soon as issued.
2. The frequency of CRL publication is specified in subsection 4.4.5.
3. New version of CP/CPSs are published as soon as they have been approved.

2.6.3 Access Controls

The online repository is available on a substantially 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance.

ASGCCA doesn't impose any access control on its Policy, its Certificate and issued certificates and CRLs.

2.6.4 Repositories

Repository of certificates is at **http://ca.grid.sinica.edu.tw/** and CRLs is at **http://ca.grid.sinica.edu.tw/CRL/** .

2.7 Compliance audit

ASGCCA may be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document.

2.8 Confidentiality

ASGCCA collects subscribers' full names , orgnization and e-mail 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.

ASGCCA does not collect any kind of confidential information.

Under no circumstances ASGCCA will have access to the private keys of any subscriber to whom it issues a certificate.

2.9 Intellectual Property Rights

Parts of this document are inspired by [CERN CA], [DOE Grid PKI], [DATAGRID-ES CA].

3 Identification and Authentication

3.1 Initial Registration

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 "Internet X.509 Public Key Infrastructure Certificate and CRL profile" [RFC 2459]. See section 7.1.4 for more details.

3.1.2 Name Meanings

The Subject Name in a certificate must have a reasonable association with the authenticate name of the entity.

3.1.3 Uniqueness of Names

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

3.1.4 Method to Prove Possession of Private Key

The public and private keys are generated on the user station when he/her fills the certificate request form with Netscape or Internet Explorer browser.

3.1.5 Authentication of Organization Identity

The RA verifies the organisation identity as member of a recognized orgnization by the ASGCCA.

3.1.6 Authentication of Individual Identity

Procedures differ if the subject is a user or a server/service:

- User :

  Subscriber must be already registered at the Academia Sinica Grid Computing Directory Service as a user defined in end entities. RA staff will check account registered on ASGCDS and contact subscriber personally.

- Host or Service certificate:

  Requests must be signed with a valid personal ASGCCA user certificate.

3.2 Routine Rekey

Rekeying of certificates can be requested by an online procedure, which check the validity of certificates.

3.3 Rekey After Revocation

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

3.4 Revocation Request

Certificate revocation request must be sent in the following ways:

- Send e-mail to asgcca@grid.sinica.edu.tw signed with a valid and trusted certificate;
- Contact personally the CA/RA staff in order to verify his/her identity and the validity of the request.

4 Operational Requirements

4.1 Certificate Application

Procedures are different if the subject is a person or a server. In every case the subject has to generate his/her own key pair. Minimum key length is 1024 bits.

- User: Certificate requests are submitted by an online procedure, using a Netscape, Mozilla or Internet Explorer browser.
- Host/Service: Certificate requests are submitted by an online procedure, using a Netscape, Mozilla or Internet Explorer browser with a valid personal ASGCCA user certificate.

4.2 Certificate Issuance

ASGCCA issues the certificate if, and only if, the authentication of the subject is successful.

If the subject is a person, a messge is sent to his/her e-mail address with the instructions on how to download it from the ASGCCA web server. In the other case, the certificate itself is sent to the address specified in the request.

If the authentication is unsuccessful, the certificate is not issued and e-mail with the reason is sent to the subject.

4.3 Certificate Acceptance

No Stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate will be revoked in the following circumstances:

- the entity's private key is lost or suspected to be compromised;
- the information in the entity's certificate is suspected to be inaccurate;
- the entity requests for revocation;
- the entity violates its obligations.

4.4.2 Who Can Request Revocation

The revocation of the certificate can be requested by:

- The certificate subscriber;
- Any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data or relation with ASGCCA.

4.4.3 Procedure for Revocation Request

The person requesting the revocation of certificate must authenticate himself in one of the following ways:

- Sending an email, signed by a valid and trusted certificate, to asgcca@grid.sinica.edu.tw, RA will contact subscriber for confirmation.
- In the other cases, authentication is performed with the same procedure used to authenticate the identity of person.

In both case above, the requesting entity must specify the reson for the revocation request and provide evidence of circumstances as described in section 4.4.1.

4.4.4 Circumstances for Suspension

The ASGCCA does not support Certificate Suspension.

4.4.5 CRL Issuance Frequency

The lifetime of the CRL is 30 days.

The CRL is updated immediately after every revocation.

CRL is reissued 7 days before expiration even if there have been no revocations.

4.4.6 Online Revocation/status checking availability

No stipulation

4.4.7 Online Revocation checking requirements

No stipulation.

4.4.8 Other forms of revocation advertisement available

No stipulation.

4.5 Security Audit Procedures Security

4.5.1 Types of Events Recorded

- Certification requests;
- Revocation requests;
- Issued certificates;
- Issued CRLs.

4.5.2 Processing Frequency of Audit Logs

No Stipulation.

4.5.3 Retention Period for Audit Logs

Logs will be kept for a minimum of 3 years.

4.6 Records Archival

4.6.1 Types of Event Recorded

The following event are stored and backed-up in safekeeping:

- certification requests
- issued certificates;
- revocation request;
- issued CRLs;
- all e-mail messages sent to ASGCCA;
- all e-mail messages sent by ASGCCA.

4.6.2 Retention Period for Archives

The minimum retention period is three years.

4.7 Key Changeover

No stipulation.

4.8 Compromise and Disaster Recovery

If the CA's private key is (or suspected to be) compromised, the CA will:

- Inform subscribers and subordinate RAs;
- Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

4.9 CA Termination

Before ASGCCA terminates its services, it will:

- Inform subscribers, subordinate CAs and cross-certifying CAs;
- Make widely available information of its termination;
- Stop issuing certificates and CRLs.
- Destroy its private key's and all copies.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

5.1.1 Site Location

The ASGCCA is located at Academia Sinica Computing Centre facilities in Taiwan.

5.1.2 Physical access

Physical access to the ASGCCA is restricted to authorized personnel.

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

Due to the location of the ASGCCA facilities floods are not expected.

5.1.5 Fire prevention and protection

ASGCCA facilities obey to the R.O.C. law regarding fire prevention and protection in buildings.

5.1.6 Media storage

The ASGCCA key is kept in several removable storage. Backup copies of CA related information are kept in removable media.

5.1.7 Waste disposal

Waste carring potentail confidential information such as old floppy disks are physically destroyed before being trashed.

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural Controls

No Stipulations.

5.3 Personnel Security Controls

All access to the servers and applications that compromise the Academia Sinica Computing Centre.

5.3.1 Background Checks and Clearance Procedures for CA Personnel

CA personnel is recruited from the Academia Sinica Computing Centre.

5.3.2 Background Checks and Security Procedures for Other Personnel

No other personnel is authorized to access ASGCCA facilities without the physical presence of CA personnel.

5.3.3 Training Requirements and Procedures

Internal training is given to CA operators.

5.3.4 Training Period and Retraining Procedures

No Stipulation

5.3.5 Frequency and Sequence of Job Rotation

Job rotation is not performed.

5.3.6 Sanctions Against Personnel

No Stipulation.

5.3.7 Controls on Contracting Personnel

No Stipulation

5.3.8 Documentation Supplied to Personnel

- Copies of this document;
- ASGCCA Operations Manual.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each subscriber must generate its own key pair. The ASGCCA does not generate private keys for subjects.

6.1.2 Private Key Delivery to Entity

The ASGCCA does not generate private keys hence does not deliver private keys.

6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to issuing CA in a secure and trustworthy manner.

6.1.4 CA Public Key Delivery to Users

CA certificate can be downloaded from the ASGCCA secure web site.

6.1.5 Key Sizes

- The minimum key length for user or host/service certificate is 1024 bits
- The CA key 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

No Stipulation.

6.1.9 Key Usage Purposes

ASGCCA private key is the only key used for signing CRLs and Certificates for person, server and service.

The Certificate key Usage field must be used in accordance with the "Internet X.509 Public Key Infrastructure Certificate and CRL profile" [RFC 2459].

6.2 Private Key Protection

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

No Stipulation.

6.2.2 Private Key Escrow

ASGCCA keys are not given in escrow. ASGCCA is not available for accepting escrow copies of keys of other parties.

6.2.3 Private Key Archival and Backup

The ASGCCA's private key is kept encrypted in multiple copies in floppy disks and CDROMs in safe places. For emergencies, the passphrase is in a sealed envelope kept in a safe.

6.3 Other Aspects of Key Pair Management

- The lifetime of ASGCCA certificate is five years.
- The lifetime of user certificate is one year.
- The lifetime of host certificate is one year.
- The lifetime of service certificate is one year.

6.4 Activation Data

The ASGCCA's private key is protected by a 15 characters passphrase.

6.5 Computer Security Controls

6.5.1 Specific Security Technical Requirements

- The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;
- Monitoring is performed to detect unauthorized software changes;
- CA systems configuration is reduced to the base minimum.

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;
- RA machines other than the signing machine are protected by a firewall.

6.8 Cryptographic Module Engineering Controls

No Stipulation.

7 Certificate and CRL Profile

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3.

7.1.2 Certificate Extensions

Basic constraints:

Not a CA.

Key usage:

Digital signature, non-repudiation, key encipherment, data encipherment.

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

7.1.3 Algorithm Object Identifiers

No Stipulation.

7.1.4 Name Forms

For Issuer:

C=TW, O=AS, CN=Academia Sinica Grid Computing Certification Authority

For User:

C=*Country-Name*, O=*Organization-Name*, OU=*OrganizationUnit-Name*, CN=*Common-Name*/ EMAIL=*Personal-Email*

example: C=TW, O=AS, OU=CC, CN=Yuan Tein Horng/emailAddress=yth@beta.wsl.sinica.edu.tw

For Host:

C=*Country-Name*, O=*Organization-Name*, OU=*OrganizationUnit-Name*, CN=*Domain-Name*

exmaple: C=TW, O=AS, OU=CC, CN=beta.wsl.sinica.edu.tw

For Services:

C=*Country-Name*, O=*Organization-Name*, OU=*OrganizationUnit-Name*, CN=*Service-Name / Domain-Name*

example: C=TW, O=AS, OU=CC, CN=FTP/beta.wsl.sinica.edu.tw

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 v1.

7.2.2 CRL and CRL Entry Extensions

No Stipulation.

8 Specification Administration

8.1 Specification Change Procedures

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

8.2 Publication and Notification Procedures

The policy is available at: **http://ca.grid.sinica.edu.tw/CPS/ .**

8.2.1 CPS Approval Procedures

No stipulation.

References

[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.doegrids.org/Docs/CP-CPS.pdf

[RFC 2459] Internet X.509 Public Key Infrastructure Certificate and CRL Profile. http://www.ietf.org/rfc/rfc2459.txt

[RFC 2527] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. http://www.ietf.org/rfc/rfc2527.txt

2.9 2.9 2.9 3.1.1, 6.1.9 1.1