Korea Institute of Science and Technology Information (KISTI) Certificate Policy and Certification Practice Statement

Version 1.1 (June 7, 2004)

Jae-Hyuck, Kwak <jhkwak@kisti.re.kr>
Sangwan Kim <sangwan@kisti.re.kr>

1. Introduction

1.1. Overview

This draft is structured based on RFC 2527 [1]. Not all sections of RFC2527 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 the Korea Institute of Science and Technology Information (KISTI) Grid Certification Authority (KISTI GRID CA) for the operations of the KISTI Grid PKI service.

The purpose of KISTI GRID CA is to issue identity and service certificates for use in Grids for its community of users and/or class of applications with common security requirements.

1.2. Community and Applicability

1.2.1. Certification Authority

KISTI GRID CA is managed by Grid Technology Research Department, KISTI Supercomputing Center.

1.2.2. Registration Authority

Grid Technology Research Department, KISTI Supercomputing Center manages the Registration Authority (KISTI GRID RA) for KISTI GRID CA.
The RA approves or rejects the certificate request for KISTI GRID CA according to the rules and procedures as identified in this CP/CPS.

1.3.3. End Entities

KISTI GRID CA issues Person, Host and Service certificates to KISTI staffs and collaborators including Korean or non-Korean people.

1.3.4. Applicability

KISTI GRID CA issues the following three types of certificate.

- Person certificates can be used to authenticate a person to relying sites that have agreed to accept certificates from KISTI GRID CA. This authentication may require the signing of Globus proxy certificates.
- Server certificates can be used to authenticate a server to relying sites that have agreed to accept certificates from KISTI GRID CA. Server certificates may be used for encryption of communication as well.
- Service certificates can be used to identify a named service on a specific host and for encryption of communication (TLS/SSL).

1.4. Contact Details

1.4.1. Specification Administration Organization

This policy was developed by, and is maintained by the Grid Technology Research Department, KISTI Supercomputing Center, Korea.

1.4.2. Contact Person

Contact point for questions related to this policy is:

Jae-Hyuck Kwak
Grid Technology Research Department, KISTI
305-806 Eoeun-dong 52, Yusung-gu, Daejeon, Korea
Phone: +82-42-869-0649
Fax: +82-42-869-0599
Email: jhkwak@kisti.re.kr

1.4.3. Person Determining CPS Suitability for The Policy

KISTI GRIDRA is responsible for setting policy, approving the CP and CPS, determination of compliance with the CPS, and oversight of activities related to the development and enforcement of policy as specified in the CP. The chair of KISTI GRID RA is:

Jae-Hyuck Kwak
Grid Technology Research Department, KISTI
305-806 Eoeun-dong 52, Yusung-gu, Daejeon, Korea
Phone: +82-42-869-0649
Fax: +82-42-869-0599
Email: jhkwak@kisti.re.kr

Sangwan Kim
Grid Technology Research Department, KISTI
305-806 Eoeun-dong 52, Yusung-gu, Daejeon, Korea
Phone: +82-42-869-0568

Fax: +82-42-869-0599
Email: sangwan@kisti.re.kr

2. General Provisions

2.1. Obligations

2.1.1. CA and RA Obligations

KISTI 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;
- Accept revocation requests according to the procedures outlined in this document;
- Authenticate entities requesting the revocation of a certificate;
- Issue a Certificate Revocation List (CRL);
- Publish the CRL issued;
- Keep audit logs of the certificate issuance process.
- Notify the RA of security incidents that have been reported and coordinate incident response between it and the RA.
- Publish contact information for the CA.
- Notify RA Points of Contact whenever contact information for the CA changes.

KISTI GRID RA will:

- Accept authentication requests from the KISTI GRID CA
- Authenticate the entity making the certification request according to procedures outlines in this document.
- Notify the KISTI GRID CA when authentication is completed for a certification or revocation request;
- Accept revocation requests according to the procedures described in this document;
- Notify the KISTI GRID CA of all revocation requests;
- Authenticate the entity making revocation request according to the procedures in this document;
- Will not approve a certificate with a life time greater than 12 months.

2.1.2. Subscriber Obligations

In all cases, subscribers will be required to:

- Read and adhere to the procedures published in this document;

- Generate a key pair using a trustworthy method;
- Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
  - For Person Certificates
    - ✓ Selecting a pass phrase of at minimum 8 characters
    - ✓ Protecting the pass phrase from others
    - ✓ Always using the pass phrase to encrypt the stored private key.
    - ✓ Never sharing the private key with other users.
  - For Service Certificates
    - ✓ Storing them encrypted whenever possible.
    - ✓ They may be kept unencrypted on the host that they represent.
- Provide correct personal information and authorize the publication of the certificate
- Notify KISTI GRID PKI immediately of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of incident.
- Use the certificates for the permitted uses only.

2.1.3. Relying Party Obligations

- Relying parties must:
  - Read the procedures published in this document.
  - Use the certificates for the permitted uses only.
  - Notify KISTI GRID PKI of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of incident.
- Relying parties may:
  - Verify that the certificate is not on the CRL before validating a certificate.

2.1.4. Repository Obligations

KISTI GRID CA will provide access to KISTI GRID CA information on its web site at:
http://ca.gridcenter.or.kr/
The information includes CA certificate, signing policy file, CRL, tools for generating certificate signing request, CP/CPS.
For providing SSL connection, the public web server uses a certificated signed internally in KISTI.

2.2. Liability

KISTI GRID PKI and its agents issue person certificates according to the practices described in this document to validate identity. No liability, implicit or explicit, is accepted. KISTI GRID PKI and its agents make no guarantee about the security or suitability of a service that is identified by a KISTI GRID 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.

KISTI GRID PKI 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 Korean government laws.

2.5. Fees

No fees are charged for issuing or renewing KISTI GRID CA certificates.
All costs for operation are covered directly or indirectly by KISTI Supercomputing Center.

2.6. Publication and Repository

2.6.1. Publication of CA information

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

- KISTI GRID CA's certificate
- Certificates issued by the PKI
- A Certificate Revocation List
- A copy of this Policy, and
- Other information deemed relevant to the KISTI GRID PKI.

2.6.2. Frequency of Publication

- Certificates must be published as soon as they are issued.
- CRLs will be published as soon as issued or refreshed once every month if there are no changes.
- All KISTI GRID PKI documents will be published to the project website as they are updated.

2.6.3. Access control

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.
KISTI GRID PKI does not impose any access control on its policy and CRL.
But it imposes an access control on its signing certificate and issued certificates. Any user want to KISTI GRID PKI is required a user subscription to the web interface system.

2.6.4. Repositories

Repository of certificates and revocation lists are at http://ca.gridcenter.or.kr/
To access to the web interface system, users require to subscribe and login the system.

2.7. Compliance Audit

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

2.8. Confidentiality

KISTI GRID CA collects subscriber's full names and email addresses. Some of this information is used to construct unique, meaningful subject names in the issued certificates.
Information included in issued certificates and CRLs is not considered confidential.
KISTI GRID PKI does not collect any kind of confidential information.
KISTI GRID PKI does not have access to or generate the private keys of a digital signature key pair, such as those used in DOE GRIDS 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 [3], [4].

3. Identification and Authentication

3.1. Initial Registration

3.1.1. Types of Names

The naming attributes of the subscriber to be requested to identify and authenticate the requester depend on the type of certificate that the subscriber requires. In the choice of the types and format of names used in the fields of CP is conforming to RFC 2459[2].

3.1.2. Name Meanings

For individuals, the value of the CN component of the DN has no semantic significance. It should have a reasonable association with the authenticated name of the subscriber. For Hosts or Services, the CN component has a structure that is defined to support SSL/TLS and the Globus software. It should include the Fully Qualified Domain Name (FQDN) of the host.

3.1.4. Uniqueness of Names

The Distinguished Name must be unique for each subject name certified by the KISTI GRID PKI. Certificates must apply to unique individuals or resources. Private keys associated with Person certificates may not be shared between people. For Hosts and Services the CN should contain the FQDN of the host.

3.2. Routine Rekey

No Stipulation

3.3. Rekey After Revocation

Rekey after revocation follows the same rules as an initial certification requeset.

3.4. Revocation request

Certificate revocation is accomplished using KISTI GRID CA web interface.

4. Operational Requirements

4.1. Certificate Application

Certificate applications can be made using KISTI GRID CA web interface. A subscribed user logins and uploads a CSR(Certificate Signing Request) and requests to the administrator.
Minimum key length is 1024 bits.

4.2. Certificate Issuance

KISTI GRID CA issues the certificate if, and only if, KISTI GRID RA has validated the identity of the requestor. Issued certificates are stored in the repository of KISTI GRID CA system which can be accessed through web interface.
If for any reasons KISTI GRID CA decides not to issue the certificate it will notify the reason for this choice to the requester.

4.3. Certificate Acceptance

No stipulation.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for Revocation

A certificate must be revoked when information in the certificate is known to be or suspected of being compromised. This includes situations where:

- The subscriber's data changed
- The subscriber's private key is compromised or is suspected to have been compromised
- The subscriber's information in the certificate is suspected to be inaccurate
- The subscriber is known to have violated his obligations

4.4.2. Who Can Request Revocation

KISTI GRID CA will accept a revocation request made by

- The holder of the certificate to be revoked

- KISTI GRID RA that validated the original certificate request
- KISTI GRID PKI managers

4.4.3. Procedure for Revocation Request

The person requesting the revocation of certificate must authenticate itself by login on the KISTI GRID CA web interface.

4.4.4. Circumstances for Suspension

KISTI GRID CA 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.

4.5. Security Audit Procedures

Security Auditing of KISTI GRID CA is not supported.

4.6. Records Archival

4.6.1. Types of Event Recorded

The following events are recorded and archived:

- Certification requests
- Issued certificates
- Issued CRLs
- All email correspondence on ca@gridcenter.or.kr

4.6.2. Retention Period for Archive

All certificate requests and confirmations are logged in the database.
The minimum retention period is 2 years.

4.7. Key Changeover

No stipulation

4.8. Compromise and Disaster Recovery

If a CA's private key is compromised or suspected to be compromised, KISTI GRID CA will:

- Inform subscribers, cross-certifying CAs and relying parties
- Terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key

4.9. CA Termination

Before KISTI GRID CA terminates its services it will:

- Inform all subscribers and subordinate RAs.
- 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 Controls

KISTI GRID PKI is located at Grid Technology Research Department, KISTI Supercomputing Center, Daejeon, Korea. The servers in KISTI Supercomputing Center are maintained in a access controlled secure racks. All access to the servers is limited to KISTI GRID PKI security staffs of KISTI Supercomputing Center. KISTI GRID PKI servers are located behind a firewall.

5.2. Procedural Controls

No stipulation

5.3. Personnel Controls

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

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

End entities' cryptographic keys are locally generated by their application during the requesting process. KISTI GRID PKI does not generate private keys for subjects.

6.1.2. Private Key Delivery to Entity

The KISTI GRID PKI never has access to the End Entity private key.

6.1.3. Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to issuing CA in a secure and trustworthy manner.
Certificate requester logins the KISTI GRID CA web interface system which runs on HTTPS-enabled web server.

6.1.4. CA Public Key Delivery to Users

CA certificate is delivered by an online transaction from a secure web server and can be downloaded using HTTPS protocol.

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

KISTI GRID CA private key is the only key used for signing CRLs and Certificates for persons, servers and services.

6.2 Private Key Protection

6.2.1 Private Key Archival and Backup

This KISTI GRID CA's private key is stored in 3DES encrypted form on the hard disk of a server separaed with the web-interface server, and is backed up by conventional server backup services and by other means. The private key is never available in plain text form (that is, in a usable form) to the server operating system or any backup service. The length of KISTI GRID CA's private key is protected by a pass phrase over 15 characters and for emergencies, the passphrase is in a sealed envelope kept ina safe.

6.3 Other Aspects of Key Pair Management

- The lifetime of KISTI GRIDCA certificate is 5 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.

7. Certificates and CRL Profile

7.1. Certificate Profile

7.1.1. Version Number

X.509 v3.

7.1.2. Certificate Extensions

BasicConstraints:

Not a CA.

KeyUsage:

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

Subject Key Identifier

Authority Key Identifier

CRL Distribution Points

Subject alternative name

Issuer alternative name

7.1.3. Algorithm Object Identifiers

No stipulation

7.1.4. Name Forms

The X.509 character set is case insensitive. But in some situations software being used to interpret these fields does interpret the name forms as case sensitive. To insure proper operation, relying parties must make sure the case used in Globus map files match the case of issued certificates. Until uniform interpretation of case is deployed it is strongly recommended that we follow the case conventions that are used in the examples below.

Issuer: C=KR, O=KISTI, CN=KISTI GRID ROOT CA

The subject name of the End Entity will be a valid Distinguished Name (DN). These DNs will consist of one of the following Relative DNs (RDN):

For People: C=KR, O=KISTI, CN=Name

For Hosts: C=KR, O=KISTI, CN=host/FQDN

For Services(LDAP): C=KR, O=KISTI, CN=ldap/FQDN

7.1.5. Name Constraints

Not supported

7.1.6. Certificate Policy Object Identifier

Currently, Object Identifier is not used.

7.2. CRL Profile

7.2.1. Version number(s)

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 KISTI GRID CA's policy and CPS.

8.2. Publication and Notification Policies

This policy is available at:
http://ca.gridcenter.or.kr/CPS/KISTI-GRID-CA-CP-CPS.pdf

8.3. CPS Approval Procedures

No stipulation

9. References

[1] RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", March 1999
http://www.ietf.org/rfc/rfc2527.txt

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

[3] DOE Grids Certificate Policy And Certification Practice Statement Version 2.4
http://www.doegrids.org/Docs/CP-CPS-V24.pdf

[4] AIST GTRC CA CP-CPS
https://sf280.hpcc.jp/CA/AIST/AIST_GTRC_CA_CP_CPS_V1.1.pdf