KEK GRID CA

Service Certificate Policy and Certification Practice Statement

Ver. 2.3.1

October 31, 2016

Computing Research Center,

High Energy Accelerator Research Organization (KEK),

Japan

Revision History Table

Date of revision or approval by the PMA	KEK GRID CA CP and CPS	Certificate and CRL Profile	Enrollment Manual
January 17, 2006 Approved by APGRID PMA	Version: 1.0.0 CP/CPS OID: 1.3.6.1.4.1.200198.1.10.2	Version: 1.0	Version: 1.0
July 7, 2006 Change in 1.3.2 and minor corrections	Version: 1.0.1 OID is not changed.		
September 26, 2007	Version: 1.10.0 CP/CPS OID: 0.2.440.200198.1.10.1.10	Version: 1.10.0	Version: 1.6
April 8, 2008	Version: 2.0.0 CP/CPS OID: 0.2.440.200198.1.10.1.2.0	Version: 2.0.0	Version: 1.7
April 13, 2009 correction of typos	Version 2.0.1 OID is not changed	Version: 2.0.1	Version: 1.7
April 16, 2009 change operations	Version 2.0.2 OID is not changed	Version: 2.0.1	Version: 1.7
Oct 8, 209 Update CP and change CP/CPS OID	Version 2.1.0 CP/CPS OID: 0.2.440.200198.1.10.1.2.1	Version: 2.1.0	Version: 1.7
Jun 28, 2010 change certificates' validity date	Version 2.1.1 OID is not changed	Version: 2.1.1	Version: 1.7
Aug 6, 2010 Update CP of CRL	Version 2.1.2 OID is not changed	Version: 2.1.2	Version: 1.7
July 1, 2013 Change contact e-mail and key length	Version 2.1.3 OID is not changed	Version: 2.1.3	Version: 1.7
January 9, 2014 Change Hash Algorithm	Version 2.1.4 OID is not changed	Version: 2.1.4	Version: 1.7
March 4, 2015 Change lifetime of CA certificate	Version 2.2.0 CP/CPS OID: 0.2.440.200198.1.10.1.2.2	Version: 2.2.0	Version: 1.7
September 24, 2015 Change RFC compliance of CRL Change limitations for username and password	Version 2.2.1 CP/CPS OID: 0.2.440.200198.1.10.1.2.3	Version: 2.2.1	Version: 1.7
May 20, 2016 Add OCSP	Version 2.3.0 CP/CPS OID: 0.2.440.200198.1.10.1.2.4	Version: 2.3.0	Version: 2.4
October 31,2016 Add Robot Certificates and minor corrections	Version 2.3.1 CP/CPS OID: 0.2.440.200198.1.10.1.2.5	Version: 2.3.1	Version: 3.2

1. Introduction

Computing Research Center (CRC) of High Energy Accelerator Research Organization (KEK), Japan, operates a Certification Authority called KEK GRID Certification Authority (CA) for Grid PKI services. Structured according to RFC 2527 [1], this document describes policy and practices of KEK GRID CA services. 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 the KEK GRID CA Policy Management Authority for the operations of the KEK GRID CA.

1.1 Overview

This document will include both the Certificate Policy and the Certification Practice Statement for the KEK GRID CA. It is the intent of the KEK GRID CA to issue Identity and server certificates for use in Grids. These certificates are for KEK researchers and their colleagues. These certificates will be compatible with the Globus middleware that is used on these Grids. The KEK GRID CA is based on NAREGI (National Research GRID Initiative) Certificate Management System.

1.1.1 Types of certificates

KEK GRID CA issues following types of certificates.

- ✓ Clients for identification
- ✓ Robots for automated service
- ✓ Globus servers
- ✓ Web servers

1.1.2 Related specification

None

1.2 Identification

KEK GRID CA uses following identifiers to identify this document and certificate policies.

Table 1-1 OIDs

OID	Object
0.2.440.200198	KEK(High Energy Accelerator Research Organization)
0.2.440.200198.1	KEK Computing Research Center (CRC)
0.2.440.200198.1.10	KEK Computing Research Center CA
0.2.440.200198.1.10.1.2.2	Certification Practice Statement
0.2.440.200198.1.10.2	CA Certificate Policy (CP)
0.2.440.200198.1.10.2.1	Globus Server CP
0.2.440.200198.1.10.2.2	Globus Client CP
0.2.440.200198.1.10.2.3	Web Server CP
0.2.440.200198.1.10.2.4	Robot CP

1.3 Community and Applicability

Client certificates can be used to authenticate a person to relying sites that have agreed to accept certificates from the KEK GRID CA. It is expected that these sites

will be collaborating with KEK. Server certificates can be used to identify a named service on a specific host. Robot certificates can be used to authenticate a service to relying sites that have agreed to accept certificates from the KEK GRID CA. These certificates may be used to authenticate the servers to another Grid entity.

1.3.1 Organization

(1) Policy Management Authority

The decision related to the management of KEK GRID CA will be performed by the coordinate committee called “KEK GRID Policy Management Authority (KEK GRID PMA)”, which consists of representatives of Computing Research Center and Information Security Office of KEK.

The KEK 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.

(2) Operating Organization

Figure 1-1 and Table 1-2 show organization and system configuration of the CA

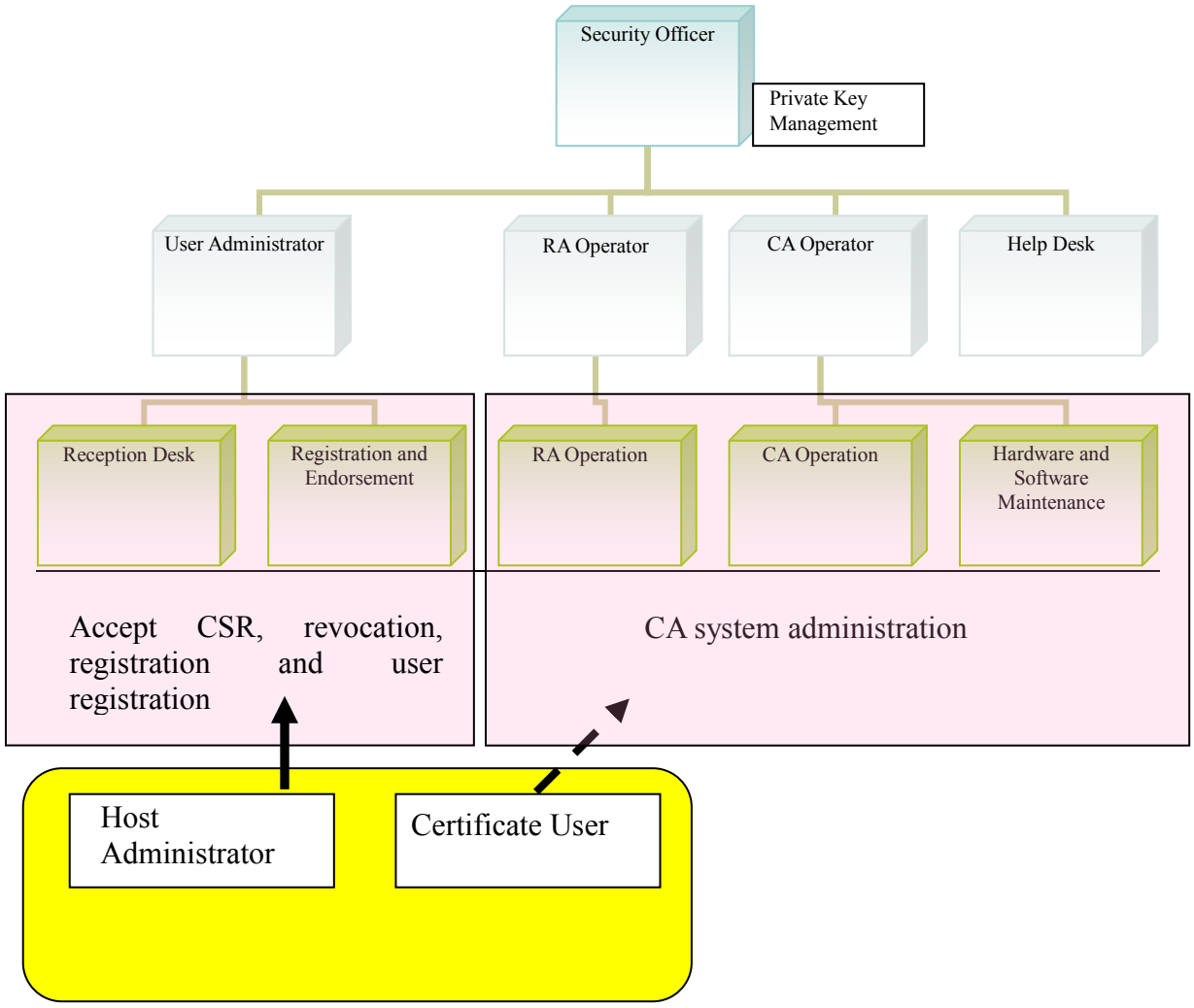

Figure 1-1 Organization and System Configuration

Table 1-2 Organization of operating CA and roles

	Main role
Security Officer	・administrates all tasks on the CA system including the CA private key
RA Operator	・creates users IDs and distribute them
CA operator	・maintains the CA system
Helpdesk	・contact point for users about CA operation
User administrator	・accepts user enrollment ・examines user information and approve the user
Certificate user	・a user using a client or robot certificate issued by KEK GRID CA
Host administrator	・an administrator of a host using a certificate issued by KEK GRID CA

RA：Registration Authority，CA：Certificate Authority

1.3.2 Applicability

It is assumed that certificates issued by KEK GRID CA have to be used for the following purposes and must not be used for any other purposes.

Table 1-3 Certificate types and their purposes

Type		**Purpose**
Client certificates		Client authentication under the GRID computing environments (SSL)
Server certificates	Globus Servers	Globus server authentication
	LCG and gLite information Servers*	Server authentication (SSL)
Robot certificates		Client authentication under the GRID computing environment (SSL) for automated service

*Only one server in every LCG (LHC Computing GRID) or gLite sites.

1.4 Contact Details

1.4.1 Specification administration organization

The KEK GRID PMA has responsibility for administrating the KEK GRID PKI services.

1.4.2 Contact information

Prof. Takashi Sasaki
Computing Research Center
High Energy Accelerator Research Organization (KEK),
1-1, Oho, Tsukuba, Ibaraki 305-0801, Japan.
Phone : +81-29-864-1171 Fax : +81-29-864-4402
E-mail : kekgridca-contact@ml.post.kek.jp

1.4.3 Person determining CPS suitability for the policy

The KEK GRID PMA has responsibility for determining CPS suitability for the policy.

2. GENERAL PROVISIONS

2.1 Obligation

2.1.1 Certification Authority obligation

The CA will:

- Create and manage the CA's private key under the secure environment.
- Issue end entity certificates based on enrollment information forwarded from the Registration Authority (RA).
- Revoke users' certificates and issue a Certificate Revocation List (CRL) based on request forwarded from the RA.
- Publish a CRL and certificate related information on a repository called KEK GRID CA repository quickly.
- Identify which CP/CPS was used to issue certificates.
- Make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data.

2.1.2 Registration Authority obligation

The RA will:

- Approve user administrators of the operating organization (KEK).
- Issue user IDs and deliver them to the user administrators.
- Forward enrollment request to the CA after the validity check using user IDs and password.
- Receive revocation request from subscribers, authenticate the origin of the request and send revocation request to the CA.
- Subscribe certificates to users in a secure and correct way.
- Archive enrollment information in the secure state.

2.1.3 Certificate user and host administrator obligation

Certificate users and host administrators shall undertake the following obligations:

- Present correct information at the enrollment.
- Procedures for the enrollment and key creation have to be performed based on the document "KEK GRID CA Enrollment Procedure Document".
- Use a certificate exclusively for authorized and legal purposes, consistent with this policy.
- Manage a certificate and its private key securely. It must not be used by other people. Protect the passphrase (private key) from others. The passphrase must be at least 12 characters long.
- Ask the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or another compromise of the subscriber's private key.
- Ask the CA to revoke the certificate when leaving the organization.
- Any end entity certificates except robot certificates must not be shared.
- Each host certificate must be linked to a single network entity.
- For a robot certificate, certificate user must generate, store and transport its private key securely according to the following criteria, and is responsible for maintaining appropriate access controls and traceability.
  - The private key must be generated on an appropriately secured computer system to which only one or more people responsible for the

robots operation have access.
- The private key must be stored on an appropriately secured computer system to which only one or more people responsible for the robots operation have access.
- The computer system must be actively monitored for security events.
- The computer system must be located in a secured room where access is controlled and limited to only authorized personnel.
- The computer system must be updated with necessary security patches.
- The private key must not be left in plaintext form for extended periods of inactivity.
- The private key must not be sent over any kind of network unprotected.
- The private key must not be sent in clear text over any kind of network.

2.1.4 Relying party obligation

Check validity of certificates and certificate chains. Issues to be checked include:

- ✓ The certificates shall not be modified,
- ✓ Within validity term,
- ✓ Checking trust CA signature,
- ✓ The certificate is not revoked.

2.1.5 User administrator obligation

User administrator will:

- Accept certificate users and host administrators, examine requests based on subscriber information which is previously registered, and approve the enrollment.

2.1.6 Repository obligation

KEK GRID CA repository will;

- Publish information specified in this CPS[2.6.1 Publication] to enable subscribers and relying parties to retrieve certificate information and CRL from the KEK GRID CA repository,
- Make efforts to operate within specified time in this CPS[2.6.2 Frequency of publication].
- Protect registered information adequately
- The KEK GRID CA repository will run on a best-effort basis, with an intended availability of 24x7.
- Operate an OCSP responder for enabling users to retrieve Certificate status information.

2.2 Liability

2.2.1 CA liability

The CA has liability:

- To issue a certificate based on the enrollment information forwarded from the RA
- To revoke a certificate based on the request forwarded from the RA.
- To register and publish client certificate information and a CRL except in time of temporary suspensions such as system maintenance or another emergent case.
- To follow practices on the procedures based on this document and have

authenticity for issued certificates. KEK GRID CA does not have liability for modification of certificates by the malicious person or compromise of the signature algorithm such as the discovery of attack.

・ To follow practices based on this document adequately so that a private key is not compromised by theft or loss.

2.2.2 RA liability

The RA has liability:

・ To send subscriber enrollment request to the CA correctly

・ To send subscriber revocation request to the CA quickly.

・ To follow practices based on this 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 compromise by theft and loss.

2.2.4 Relying party liability

No Stipulation

2.2.5 User administrator liability

User administrator has liability to ensure that enrollment information to the CA is correct.

2.2.6 Repository liability

KEK GRID CA repository has liability

・ To respond to retrieval requests within operating time defined in this document.

・ Not to have the liability that the stored CRL is not the latest one at the time of the retrieval request.

2.3 Financial Responsibility

KEK GRID CA assumes no financial responsibility for use or management of any issued certificate.

2.4 Interpretation and Enforcement

Interpretation of this CP and CPS is made according to Japanese laws**.**

2.5 Fees

No fees are charged for KEK GRID CA certificates.

2.6 Publication and Repository

2.6.1 Publication

The following information will be published on the KEK GRID CA repository:

- Client certificate information used for GRID map file
- A CRL issued by KEK GRID CA

- The CA’s certificate
- The CA’s certificate’s fingerprint
- The CA’s signing policy file
- A copy of this policy
- Other information deemed relevant to the KEK GRID CA

2.6.2 Frequency of publication

- Certificates information will be published on the KEK GRID CA repository as soon as issued.
- CRLs will be published as soon as issued or refreshed on scheduled update.
- All KEK GRID CA documents will be published on the KEK GRID CA repository 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 control

The information specified in this document [2.6.1 Publication] is accessible through KEK network under adequate access control.

2.6.4 Repository

The information specified in this document [2.6.1 Publication] is stored in the KEK GRID CA repository and accessible from KEK network.

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

The KEK GRID CA will accept at least one external audit a year.
Besides, the KEK GRID CA performs a self-audit by the CA and RA staff at least once per year according to this document.

2.7.2 Identity/Qualifications of auditor

The CA will be audited by other cross-certifying CAs.

2.7.3 Auditor's relationship to audited party

Desirable auditors are third-parties to the KEK GRID CA.

2.7.4 Topics covered by audit

The audit will focus on whether the operation of the KEK GRID CA is compliant to this document and the Minimum CA Requirements specified by the Asia Pacific Grid Policy Management Authority.

2.7.5 Actions taken as a result of deficiency

The KEK GRID PMA will decide the necessary actions identified in the audit and submit the report to the auditor in a timely manner.

2.7.6 Communications of results frequency of entity compliance

The results of the audit will be informed to the KEK GRID CA operation staff. The KEK GRID PMA releases the results to policy management authorities of their cross-certifying CAs as necessary.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

Except explicit information specified in CPS [2.6.1 Publication], all related information will be treated as confidential. Confidential information will not be provided to any other people. Confidential information including documents and electronic media will be stored securely by the KEK GRID CA Security Officer.

2.8.2 Types of information that are not considered confidential

The information specified in CPS [2.6.1 Publication] is not confidential information in this system.

2.8.3 Disclosure of certificate revocation/suspension information

When a certificate is revoked by the CA, the revocation date and reason will be published. Other detailed information is not confidential but 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

The 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

KEK GRID CA does not claim any intellectual property rights on issued certificates. Parts of this document are inspired by CP/CPS documents of CERN CA[2], GridCanada CA[3], ASGC CA[4], NAREGI CA[5] and AIST CA[6].

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Type 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[7]). See section 7 for more details.
For a robot certificate, the CN must be “Robot:” string followed by a meaningful service description and full name of the certificate user. Service description and certificate user's name must be separated by " - ", e.g. "CN=Robot: Noname service - John Doe". Also, the Subject Alternative Names extension must include an e-mail

address of the certificate user.

3.1.2 Need for names to be meaningful

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

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 Distinguished Name must be unique for each subject name certified by the KEK GRID CA. For client and robot certificates, each CN component will include the full name of the certificate user. For hosts and services, the CN must contain the fully qualified domain name (FQDN) of the host.
Certificates must apply to unique individuals or resources.

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 RA verifies the organization identity as a member of a recognized organization by the KEK GRID CA.

3.1.9 Authentication of individual identity

The KEK GRID CA verifies the identity of an applicant as described below:

- The person must be an existing user of KEK CRC *i.e.,* the person must have an account on either of the KEK CRC computing facilities.
  - One referee among KEK employees is requested.
  - The person must be a member of either of the projects at KEK.
- A copy of his/her personal identification document with a photo must be attached to his/her application form.

A KEK staff in the position of RA will verify the identification by meeting him/her in person. For those who have a proper reason why they cannot show up at the RA office, an interview on the TV conference system can be substitutable with the process.

3.2 Routine Rekey

Rekeying a certificate can be requested by an on-line procedure, which checks the validity of the certificate. KEK GRID CA does not allow renewing an end entity certificate. Therefore subscribers must take the rekeying procedure. A KEK staff in the position of RA will verify the identification.

3.3 Rekey after Revocation

Rekey after revocation follows the same rules as an initial registration as described in section 3.1

3.4 Revocation Request

When revocation of a certificate is requested to the KEK GRID CA, the subscriber identity and organization shall be verified as when issuing a certificate according to section 3.1 of this document.

3.5 CA's Transition Procedure

KEK CA has the following planned procedure about the transition of the CA's cryptographic data.

(1) KEK GRID CA changes the CA key for responding the signing request of new end entity certificate.

(2) KEK GRID CA continues using the old key only for revoking certificates and signing the updated CRL.

(3) After the CA's key is changed, KEK GRID CA system provides two CA certificates and two CRLs which are signed by old key and by new key respectively, through CA repository.

(4) After the old CA certificate expires, KEK GRID CA system will terminate to provide the old CA certificate and the CRL signed by the old key.

4. OPERATIONAL REQUIREMENTS

This chapter describes requirements for end entity certificates, not defined for CA self-signed certificate.

4.1 Certificate Application

(1) Certificate application

Certificate user or host administrator must submit an application form to the RA by paper documents. User administrator of the RA examines the request according to this document [3.1.9 Authentication of individual identity]. If the application is approved, then the RA will inform the CA that the request has been approved. Paper documents are brought by hand from the RA to the CA. Then, the CA will issue a username and an initial password (that consists of random characters), and the issued username and password are recorded on the paper and sent to the applicant by postal mail or FAX. The applicant is requested to change the initial password to new one which must be at least ten characters long. The username and password are used for obtaining a certificate from the CA server on-line. Detailed procedure for the certificate application is described in "KEK GRID CA Enrollment Manual" which is available on the KEK GRID CA repository.

(2) Certificate enrollment

Certificate user or host administrator needs to create a key pair on his/her machine according to the procedures described in "KEK GRID CA Enrollment Manual", and sends a certificate signing request that 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 "KEK GRID CA Enrollment Manual" which is available on the KEK GRID CA repository.

4.2 Certificate Issuance

Subscribers are provided with an enrollment tool which creates a key pair and a CSR and supports LCMP (Lightweight Certificate Management Protocol) which enables

secure communication with the KEK GRID CA system.

4.2.1 Receipt certificate enrollment

RA will execute the following steps after receipt of end entity certificate request.

- Prompt the subscriber to input the username and password, and a one-time license ID in case of server or robot certificate.
- Verify the username and password, and the license ID if any.
- Accept enrollment information which will be subject information in the certificate.

4.2.2 Issuance certificate

An RA administrator checks the certificate signing request whether it is valid or not. If the request is valid, the administrator sends the certificate signing request to the CA server using a secure connection that is a dedicated path between the RA server and the CA server. The CA server will issue a certificate signed with the CA private key and the subscriber's public key for the issue request received from the RA server.
After the CA server issues a certificate, the subscriber will be notified by e-mail that the certificate has been issued.

4.2.3 Subscribe certificate

Subscribers receive the certificate through the RA server.

4.3 Certificate Acceptance

Certificate user and host administrator will register the certificate to the certificate stores based on the user's operational document.

4.4 Certificate Suspension and Revocation

The procedure for revocation request from a subscriber or the CA can, as for certificate enrollment, be done on-line using the Lightweight Certificate Management Protocol (LCMP), or the web enrollment functions provided in standard Windows environments. All communications are encrypted.

4.4.1 Circumstances for revocation

In any of the following circumstances, a certificate will be revoked due to a subscriber's request or by the CA.

- End entity's key is compromised or suspected of being compromised.
- End entity information in the certificate is suspected of being incorrect.
- Subscriber violates his/her obligations, as specified in section [2.1.3 Certificate user and host administrator obligation] of this CPS.
- The CA private key is suspected of being compromised.
- When the use of the certificate stops (including the resignation of the subscriber, etc.).
- The CA private key is compromised.

4.4.2 Who can request revocation

Subscribers, the KEK GRID RA and the KEK GRID CA can request revocation.

4.4.3 Procedure for revocation request

Subscribers will send revocation request based on the operational document provided when revocation circumstances occur. RA server will authenticate the requester as described in this document [**3.4 Revocation Request**]. Then RA server sends revocation request to CA server. The CA server will revoke the certificate and update the signed CRL on the KEK GRID CA repository.
When a certificate is revoked, the subscriber of the certificate will be notified of the revocation by e-mail.

4.4.4 Revocation request grace period

The KEK GRID CA processes revocation as soon as it receives the request. The revocation information will be published on the KEK GRID CA repository.

4.4.5 Circumstances for suspension

The KEK GRID CA does not support certificate suspension.

4.4.6 Who can request suspension

The KEK GRID CA does not support certificate suspension.

4.4.7 Procedure for suspension request

The KEK GRID CA does not support certificate suspension.

4.4.8 Limits on suspension period

The KEK GRID CA does not support certificate suspension.

4.4.9 CRL issuance frequency

The KEK GRID CA refreshes the CRL and publishes it on the KEK GRID CA repository according to the revocation requests and the expiration of the CRL. CRL validity term is shown in Table 4-1.
KEK GRID CA issues a new CRL immediately after a revocation or at least seven days before the expiration date.

Table 4-1 CRL Issuance interval

	CRL
Issuer CA	KEK GRID CA
CRL validity	30days

4.4.10 CRL checking requirements

Relying party verifies a certificate by retrieving the newest CRL from the KEK GRID CA repository.

4.4.11 On-line revocation/status checking availability

On-line revocation information is available from the OCSP responder. The OCSP responder reloads the CRL every hour.

4.4.12 On-line revocation checking requirements

No stipulation

4.4.13 Other forms of revocation advertisements available

No stipulation

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation

4.5 Security Audit Procedures

The KEK GRID CA will retain records as much as possible so that the KEK 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

The following information will be recorded by the KEK GRID CA. For each record, the event type, date and time, and occurrence information (system name, operations staff name, etc.) will be included.

- CA: Server log
- CA: Server access log
- CA: Certificate and CRL issuance and revocation log
- CA: Error log
- CA: OS Login, Logout, Reboot log
- RA: Server log
- RA: Server access log
- RA: CRL publisher activity log
- RA: CRL publisher error log
- RA: Certificate issuance, revocation log
- RA: Error log
- RA: OS Login, Logout, Reboot log
- HSM log
- Token access log
- Machine room work record
- Key sign-out journal

4.5.2 Frequency of processing logs

No stipulation

4.5.3 Retention period for audit logs

The minimum retention period is three years.

4.5.4 Protection of audit logs

Access logs and system logs are protected by the authorization mechanism provided by UNIX operating system. Only the owners of these logs are able to modify the logs. Access logs and system logs are periodically backed up to the removable media which are stored in a lockable cabinet when it is off-line. For logs of physical access to the CA room, 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 room are stored

in a lockable cabinet.

4.5.5 Audit log backup procedures

CA operators will obtain each type of log recorded by the CA server and other systems on external media weekly, and store them monthly.

4.5.6 Audit collection system

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 recorded

The KEK GRID CA will store the following archive data. Documents will be stored including all versions and their revision history.

- All certificates and CRLs issued by the KEK GRID CA
- All enrollments submitted by subscribers and any notifications sent to subscribers
- Work record related to the CA key
- The audit logs as specified in section [4.5.1 Types of event recorded] of this CPS
- Conformance audit and security audit records
- Certificate use rules and guides provided to subscribers
- This document and operational procedure documents
- Other important materials related to decisions of the KEK GRID CA PMA
- OCSP responder logs

4.6.2 Retention period for archive

Archived data will be stored for three years. In addition, the identity validation records will be kept as long as there are valid certificates based on such a validation.

4.6.3 Protection of archive

Section 4.5.4 of this document specifies how the archive logs are to be protected. Archival data will be protected in a lockable cabinet with appropriate entry control, and the CA operator will manage sign-out of the cabinet key.

4.6.4 Archive backup procedures

The electronic part of the records is archived daily on removable media. The paper-based archives are stored in a lockable cabinet at KEK.

4.6.5 Requirements for time-stamping of records

All on-line archives are time-stamped using a host clock that is synchronized with NTP. Date and time are recorded in the paper-based archives manually.

4.6.6 Archive collection system

No stipulation

4.6.7 Procedures to obtain and verify archive information

No stipulation

4.7 Key Changeover

4.7.1 End entity certificate validity term

Each type of end entity certificate has to be re-issued in the following validity term.

Table 4-2 validity terms of end entity certificates

Type		Validity
Client certificate		400 days
Server certificate	Globus servers	400 days
	Web servers	400 days
Robot certificate		400 days

4.7.2 CA certificate validity term

The CA will stop signing new end entity certificate by its private key when its validity is shorter than that of end entity certificate. CA certificate validity term is 20 years.

Table 4-3 CA certificate validity

Type	Validity
KEK GRID CA	20 years

4.8 Compromise and Disaster Recovery

4.8.1 Computing resources, software, or data are corrupted

If it is detected that hardware, software or data are corrupted or damaged, it is necessary to recover the system by using backup data immediately.

4.8.2 CA private key is compromised

If it is suspected that CA private key is compromised, it is necessary to revoke certificates based on the CPS and to re-build the new KEK GRID CA system.

- Terminate PKI service if the HSM (Hardware Security Module) is stolen or its operational key is lost, and announce the fact to all related parties.
- Revoke all end entity certificates so that any relying party does not trust the CA.
- If a person in charge of all CA system management decides that it is difficult to use the same private key continuously, revoke the CA certificate by the key. After recognition of secure circumstances for CA system, re-create a key pair and re-build the CA system.

4.8.3 Secure facility after a natural or another type of disaster

The system needs to be recovered according to [4.8.1 Computing resources, software, or data are corrupted].

4.9 CA Termination

The KEK GRID CA will inform any related parties ahead of time regarding termination of the CA operations and preservation of related backup data, etc., before the prescribed procedures for termination are carried out.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The KEK GRID CA system will be located where it is not easily susceptible to damage from water exposure, earthquake, fire or other disasters. It will be constructed to be earthquake and fire resistant, and with safety measures to prevent unauthorized entry. A safe location shall also be provided to protect CA machinery from damage or unauthorized entry.

5.1.2 Physical access

The room, in which the CA server is located, is locked by a mechanical lock and physical access to the room is restricted to explicitly authorized persons documented in [**5.2 Procedural Controls**]. A CA operator is not allowed to enter the room alone and needs to enter the room with another CA operator. If a CA operator needs to enter the room alone, he/she must notify the fact to the Security Officer by e-mail before and after entering the room. All events about the access to the room must be recorded in the paper sheets prepared in the room. The event records 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 power for the server machines is taken from the uninterruptible power supply (UPS).

The machine room is equipped with adequate air conditioning to maintain a comfortable environment for the servers and other devices, and for the CA staff to perform their duties.

5.1.4 Water exposures

No special countermeasure.

5.1.5 Earthquake and protection

A building is earthquake resistant construction and has countermeasures against equipment to fall down.

5.1.6 Fire prevention and protection

A building is fire-resistant construction, and the room is fire prevention cell with fire protection.

5.1.7 Media storage

Media will be stored in the lockable cabinet in the room where adequate access control is done.

5.1.8 Waste disposal

Adequate waste disposal process for the document or media containing confidential information is followed.

5.2 Procedural Controls

5.2.1 Trusted roles

The staff is assigned trusted roles as defined in section 1.3 of the document.

5.2.2 Number of persons required per task

Organization of the KEK GRID CA is described in this document [1.3.1 Organization], and the number of persons for each task is described in this section. KEK GRID CA service is operated by:

- Two Security Officers
- Two RA Operators
- Two CA Operators
- One User Administrator.

No one works for different tasks, i.e. the KEK GRID CA service is operated by seven staffs. Besides these staffs, four other persons in Help Desk of KEK Computing Research Center will work as Help Desk staff of the CA.

5.2.3 Identification and authentication for each role

The system will identify and authenticate the operator when the staff operates the system.

5.3 Personnel Controls

All of the personnel controls are based on another document.

5.3.1 Background check procedures

The role of the CA requires a well-trained person who is familiar with the PKI and technically competent. There are no background checks.

5.3.2 Training requirements

No stipulation

5.3.3 Retraining frequency and requirements

No stipulation

5.3.4 Job rotation frequency and sequence

No stipulation

5.3.5 Sanctions for unauthorized actions

No stipulation

5.3.6 Contracting personnel requirements

No stipulation

5.3.7 Document supplied to personnel

The KEK GRID CA provides an internal instruction manual for personnel.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

(1) CA key

A CA key pair is generated using Hardware Security Module (HSM) by the Security Officer.

(2) End entity key

An end entity key pair is generated by software on each subscriber's terminal at the time of enrollment.

6.1.2 Private key delivery to end entity

The CA system does not deliver an end entity private key since the key is generated at the end entity.

6.1.3 Public key delivery to CA

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

6.1.4 CA public key delivery to users

The CA certificate will be published on the KEK GRID CA repository.

6.1.5 Key sizes

Table 6-1 shows the key algorithm and length for each type of key.

Table 6-1 Algorithm and key length

type		**Algorithm and key length**
CA key		SHA1 with RSA 2048bits
End entity key	Client	SHA512 with RSA 2048bits
	Robot	SHA512 with RSA 2048bits
	Server	SHA512 with RSA 2048bits

6.1.6 Public key parameters generation

No stipulation

6.1.7 Parameter quality checking

No stipulation

6.1.8 Hardware/software key generation

As defined in this document [6.1.1 Key pair generation].

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

A private key for end entity is used for digital signature, non repudiation, key

encipherment, and data encipherment. This purpose will be set in the extension field of “keyUsage” of the end entity certificate.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

The CA private key is protected by HSM compliant with FIPS140-2 Level3.

6.2.2 Private key (n out of m) multi-person control

The CA’s private key is not under (n out of m) multi-person control. But the KEK GRID CA implements multi-person control for the access to the CA server as described in this document [5.1.2 Physical access]. A backup copy of the CA’s private key is under (2 out of 3) multi-person control.

6.2.3 Private key escrow

Not perform

6.2.4 Private key backup

(1) CA private key backup
The CA private key will be backed up into a token in secure places where access is controlled. Backup is made by the CA operators and the Security Officer.
(2) End entity private key backup
It remains up to users to backup and manage their private keys.
(3) Passphrase of the CA private key backup
The passphrase of the CA private key will be kept in sealed envelope. The KEK Grid PMA staff will keep this sealed envelope in a safe place.

6.2.5 Private key archival

The CA private key is not archived.

6.2.6 Private key entry into cryptographic module

The CA private key is created in the HSM and securely stored by the Security Officer with the CA operator. The CA private key is protected with a passphrase of at least 15 characters. The passphrase is known by only the Security Officer and the CA operators. End entity private key is created according to ”KEK GRID CA Enrollment Manual” which is available on the KEK GRID CA repository. To register the CA private key recovered from backup media needs approval by the Security Officer and must be performed under multi-person control.

6.2.7 Method of activating private key

The CA private key in HSM will be activated by a Security Officer or a CA operator.

6.2.8 Method of deactivating private key

The CA private key will be deactivated in the server by a Security Officer.

6.2.9 Method of destroying private key

No stipulation

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

No stipulation

6.3.2 Usage periods for the public and private keys

Usage periods for the public and private keys are described in this CPS [4.7.1 End entity certificate validity term] and [4.7.2 CA certificate validity term].

6.4 Activation Data

6.4.1 Activation data generation and installation

Activation data consist of physical keys and a passphrase, which is set/input by a Security Officer or a CA Operator. Physical access to the CA server is described in this document [5.1.2 Physical access].

6.4.2 Activation data protection

Passphrase as activation data will be protected from use and modification defined in the other rule.

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

CA server is dedicated to the CA operation.

6.5.2 Computer security rating

No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System development controls

No stipulation

6.6.2 Security management controls

No stipulation

6.6.3 Life cycle security ratings

No stipulation

6.7 Network Security Controls

The CA server and the RA server will be on-line and appropriately protected by the firewall. It is securely protected from wrong penetration access except for access to the

KEK GRID CA repository and communication path between RA and CA.

6.8 Cryptographic Module Engineering Controls

No stipulation

7. CERTIFICATE, CRL, AND OCSP PROFILES

The CRL of KEK GRID CA is compliant with RFC5280.
The profile for OCSP of KEK GRID CA is compliant with RFC2560.

7.1 Certificate Profile

Certificate profile is described in a separate document, “KEK GRID CA Certificate and CRL Profile version 2.3.1”. The document is available on the KEK GRID CA repository.

7.2 CRL Profile

CRL profile is described in a separate document, “KEK GRID CA Certificate and CRL Profile version 2.3.1”. The document is available on the KEK GRID CA repository.

7.3 OCSP Profile

7.3.1 OCSP version

The KEK GRID CA provides Version 1 OCSP responses.

7.3.2 OCSP extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

The KEK GRID PMA will change this document by necessity. Revision is made and approved by the KEK GRID PMA. Minor editorial changes to this document can be made without approval by the KEK 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 KEK GRID PMA. New OID will be assigned to the revised document for such substantial changes would be made.

8.2 Publication and Notification Policies

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

8.3 CPS Approval Procedures

All major changes must be approved by the KEK GRID PMA. Change logs are described in Appendix A of this document.

9. Glossary

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 the 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, which 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, robot and service certificates).

FIPS

American Federal Information Processing Standards Publication. FIPS140-2 is a standard for evaluating cryptographic modules.

Host Certificate

A certificate for server certification and encryption of communications (SSL/TLS). It will represent a single machine.

gLite

The name of Middleware developed in the European Union.

LHC

Large Hardon Collider, the facility at CERN, Switzerland.

LCG

LCG stands for LHC Computing GRID, and is the name of the project and its middleware. The LCG middleware is based on gLite.

Online Certificate Status Protocol (OCSP)

An Online Certificate Status Protocol is an Internet protocol used for obtaining the revocation status of the certificate.

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 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.

Robot Certificate

A certificate for an unattended service or process running on behalf of a person.

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 engine.

Appendix A. Change Logs

- Version 0.3 to Version 1.0
  - Major revision according to the minimum CA requirement of APGRID PMA

References:

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

[2] CERN Certification Authority – Certificate Policy and Certification Practice Statement, Document OID 1.3.6.1.4.1.96.10.1.2.3, November 8, 2004.

[3] Grid Canada Certificate Policy and Certification Policy Statement, Document OID 2.16.124.101.1.274.47.1.1, December 20, 2002.

[4] Academia Sinica Grid Computing Certification Authority (ASGCCA) Certificate Policy and Certification Practice Statement, OID 1.3.6.1.4.1.5935.10.1.1.1, June 2003.

[5] NAREGI Certificate Practice Statement Ver1.0.1, OID 1.2.392.00200181.1.1, September 27, 2005

[6] 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

[7] R. Housley, W. Ford, W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2459, January 1999.

[8] EU GridPMA Guideline on IGTF Approved Robots, OID: 1.2.840.113612.5.4.1.1.1.6, September 2014.