KEK GRID CA

Service Certificate Policy and Certificate Practices Statements

Difference between Ver. 1.10.0 and Ver. 2.0.0.

April 2, 2008

Computing Research Center,

High Energy Accelerator Research Organization (KEK),

Japan

1 Revision History Table

We added information of new version in the last line of the **Revision History Table**.

Ver. 1.10.0 (Current Version)

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 no 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
January 18, 2008	Version: 1.10.1 CP/CPS OID: 0.2.440.200198.1.10.1.10	Version: 1.10.1	Version: 1.7

Ver. 2.0.0 (Proposal Version)

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 no 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

2 Identification

We modified OID of "Certification Practices Statements", "Globus Server CP", "Globus Clients CP" and "Web Server CP" in the **Table 1-1**.

Ver. 1.10.0 (Current Version)

Table1-1 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
0.2.440.200198.1.10.1.1.10	Certification Practices Statements
0.2.440.200198.1.10.2	CA Certificate Policy (CP)
0.2.440.200198.1.10.2.1.1.10	Globus Server CP
0.2.440.200198.1.10.2.2.1.10	Globus Clients CP
0.2.440.200198.1.10.2.3.1.10	Web Server CP

Ver. 2.0.0 (Proposal Version)

Table1-1 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
0.2.440.200198.1.10.1.2.0	Certification Practices Statements
0.2.440.200198.1.10.2	CA Certificate Policy (CP)
0.2.440.200198.1.10.2.1.2.0	Globus Server CP
0.2.440.200198.1.10.2.2.2.0	Globus Clients CP
0.2.440.200198.1.10.2.3.2.0	Web Server CP

3 Uniqueness of names

We modified the sentence in the section **"3.1.4 Uniqueness of names"**.

Ver. 1.10.0 (Current Version)

The Distinguished Name must be unique for each subject name certified by the KEK GRID CA. Each CN component will include the full name of the subscriber.
For hosts and services the CN should contain the fully qualified domain name (FQDN) of the host.
Certificates must apply to unique individuals or resources. Users must not share certificates

Ver. 2.0.0 (Proposal Version)

The Distinguished Name must be unique for each subject name certified by the KEK GRID CA. Each CN component will include the full name of the subscriber.
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. Users must not share certificates

4 Routine Rekey

We added the sentence in the section “3.2 Routine Rekey”.

Ver. 1.10.0 (Current Version)

Rekeying of certificates can be requested by an online procedure, which checks the validity of certificates. A KEK staff in the position of RA will verify the identification.

Ver. 2.0.0 (Proposal Version)

Rekeying of certificates can be requested by an online procedure, which checks the validity of certificates. KEK Grid CA does not allow re-new of end entity certificates, therefore users must use re-key procedure. A KEK staff in the position of RA will verify the identification.

5 CA’s transition procedure

We added the section **“3.5 CA’s transition procedure”**.

Ver. 1.10.0 (Current Version)

(No description in Ver. 1.10.0.)

Ver. 2.0.0 (Proposal Version)

3.5 CA’s transition procedure

KEK CA has the below planed procedure about transition of the CA's cryptographic data.

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

(2) KEK GRID CA continues to use the old key only for revoking certificates and the signing CRL updates.

(3) After the CA's key is changed, KEK GRID CA system continues to provide two ca certifications and to update two CRLs which are signed by current key and by new key respectively through CA's web site.

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

6 Retention period for archive

We added the section **“4.6.2 Retention period for archive”**.

Ver. 1.10.0 (Current Version)

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.

Ver. 2.0.0 (Proposal Version)

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.

7 CA certificate validity

We modified the period of the CA certificate validity in the section **"4.7.2 CA certificate validity"**.

Ver. 1.10.0 (Current Version)

The CA will stop to sign new user certificates by its private key before it is shorten than user certificates. CA certificate validity is 5years

Table4-4 CA certificate validity

Type	Validity
KEK GRID CA	5 years

Ver. 2.0.0 (Proposal Version)

The CA will stop to sign new user certificates by its private key before it is shorten than user certificates. CA certificate validity is 10 years

Table4-4 CA certificate validity

Type	Validity
KEK GRID CA	10 years

8 Private key backup

We added the description in the section **"6.2.4 Private key backup"**.

Ver. 1.10.0 (Current Version)

(1) Private key backup

The private key will be back-up into a token in secure places where access is controlled. Back-up is made by the CA operators and the Security Officer.

(2) End entity private key back up

It remains users to private key back up and management.

Ver. 2.0.0 (Proposal Version)

(1) Private key backup

The private key will be back-up into a token in secure places where access is controlled. Back-up is made by the CA operators and the Security Officer.

(2) End entity private key back up

It remains users to private key back up and management.

(3) Pass phase of the CA private key back up

The pass phrase 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.

9 CERTIFICATE AND CRL PROFILES

We added the sentence in the section **"7 CERTIFICATE AND CRL PROFILES"**.

Ver. 1.10.0 (Current Version)

(No description in Ver. 1.10.0.)

Ver. 2.0.0 (Proposal Version)

The CRL of KEK Grid CA is compliant with RFC3280.