HKU Grid Certification Authority Certificate Policy and Certification Practice Statement

Version: 3.0

Information Technology Services, The University of Hong Kong

9 February 2018

DOCUMENT HISTORY

Document Name	Document Version	Status	Date	By whom	Review	Remarks
HKU Grid CA CP/CPS	1.0	Created	20 Apr 2009	Frankie Cheung	Kwan Wing Keung	Reviewed by APGridPMA
HKU Grid CA CP/CPS	1.1	Updated	22 Mar 2011	Lilian Chan	Kwan Wing Keung	Approved
HKU Grid CA CP/CPS	2.0	Updated	8 Mar 2012	Lilian Chan	Kwan Wing Keung	Reviewed by APGridPMA
HKU Grid CA CP/CPS	2.1	Updated	20 Mar 2014	Lilian Chan	Kwan Wing Keung	Approved
HKU Grid CA CP/CPS	3.0	Updated	9 Feb 2018	Lilian Chan	Kwan Wing Keung	Reviewed by APGridPMA

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

Information Technology Services (formerly known as Computer Centre), the University of Hong Kong, is an IT service provider to its university members for teaching and research. This document is the combined Certificate Policy and Certification Practice Statement of the HKU Grid Certificate Authority. It describes the set of procedures followed by the HKU Grid CA and is structured according to RFC 3647. Sections that are not included have a default value of "No stipulation". The rules & procedures in the document are approved by the HKU Grid Policy Management Authority (HKU Grid PMA).

1.2 DOCUMENT NAME AND IDENTIFICATION

Document Title: **HKU Grid Certificate Authority Certificate Policy and Certification Practice Statement**

Document Version: **3.0**

Document Date: **9 February 2018**

CP OID: **1.3.6.1.4.1.30850.2.2.40000.2.1.3.0**

CPS OID: **1.3.6.1.4.1.30850.2.2.40000.2.2.3.0**

The OID is constructed as shown in the table below:

The University of Hong Kong	1.3.6.1.4.1.30850
Project Document	.2
Product Document	.2
Information Technology Services	.40000
GRID CA	.2
CP/CPS	.1/2
Major Version	.3
Minor Version	.0

1.3 PKI PARTICIPANTS

1.3.1 Certificate Authorities

The HKU Grid CA does not issue certificates to subordinate Certificate Authorities.

1.3.2 Registration Authorities

The HKU Grid CA delegates the authentication of individual identity to Registration Authorities (RA). RAs must sign an agreement with the HKU Grid CA, stating their adherence to the procedures described in this document. The following is the HKU Grid RA registration procedure:

- RA applicant must accept the CP/CPS and agree to all RA responsibilities.
- RA applicant must be an employee of the institution or organization involving in Grid research & scientific collaborations with HKU
- RA applicant has to provide photo, work ID and proof of work.
- Complete the RA application form and fax it to HKU Grid CA.
- Send verification e-mail to HKU Grid CA.
- HKU Grid CA will then arrange face to face meeting with the RA applicant.
- RA applicant has to apply for HKU Grid CA User certificate.
- After completing the request, HKU Grid CA will publish the RA contact information on HKU Grid CA website.

1.3.3 Subscribers (End Entities)

HKU Grid CA issues certificates for the following subjects:

- Regular staff and students of The University of Hong Kong (HKU).
- Other collaborators or institutes can provide valid official documents as the proof of the involvement in Grid research & scientific collaborations with HKU.

The term end entity is used to refer to the holder of the private key. For a person certificate it will be the subscriber, but for a host certificate and OCSP responder certificate the end entity may be some process running on a machine.

HKU Grid CA issues OCSP responder certificate to servers operated by HKU Grid CA only.

The subscriber is 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 user certificates

- select a pass phrase of at least 12 characters
- protect the pass phrase from others
- always use the pass phrase to encrypt the stored private key
- protect the private key in accordance with "Guidelines on Private Key Protection" (OID 1.2.840.113612.5.4.1.1.1.5.4).

- for host certificates
  - store them in encrypted form whenever possible
  - provide correct information and authorize the publication of the certificate.
  - use the certificates for the permitted uses only.

1.3.4 Relying Parties

HKU Grid CA's relying parties includes the following:

- Employees of HKU Information Technology Services or collaborating research institutes in Hong Kong.
- Other collaborators or institutes having the involvement in Grid research & scientific collaborations with HKU.

Relying parties' obligations are as follows:

- Must read the procedures published by the HKU Grid CA.
- Must use the certificates for the permitted uses only.
- Must notify HKU Grid CA of any security incidents.

1.3.5 Other Participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Certificates from HKU Grid CA may be used in applications for the following purposes:

- For purposes of authentication, digital signature and data encryption in Grid computing & scientific research.
- Certificates may also be used to satisfy other general or specific requirements of Grid computing.

1.4.2 Prohibited Certificate Uses

Certificates issued by the HKU Grid CA must not be used for:

- Electronic commerce
- Military usage

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

This policy is developed and maintained by HKU Grid Policy Management Authority (HKU Grid PMA) at Information Technology Services, the University of Hong Kong.

1.5.2 Contact Person

Miss Lilian Chan Yuk Lin
HKU - ITS/HPC Team
Phone: +852-39172485
Fax: +852-25597904
Email: gridca@hku.hk
Address: Information Technology Services, The University of Hong Kong, Pokfulam, Hong Kong

1.5.3 Person Determining CPS Suitability for the Policy

See section 1.5.2.

1.5.4 CPS Approval Procedures

HKU Information Technology Services is responsible for the CP and CPS.

For the global Grid collaborations, HKU Information Technology Services is a member of APGrid PMA.

Major changes must be approved by the APGrid PMA Community.

Minor changes can be done by HKU Grid PMA & should be notified through APGrid PMA mailing list.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 General Definitions

The following definitions and associated abbreviations are used in this document.

HKU	The University of Hong Kong

ITS	Information Technology Services, the University of Hong Kong
HPC	High Performance Computing
Certificate	Synonymous with Public Key Certificate.
Certificate Authority (CA)	An entity trusted by one or more users to create and assign public key certificates, and be responsible for the keys during their whole lifetime.
HKU Grid CA	HKU Grid Certificate Authority
HKU Grid PMA	HKU Grid Policy Management 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.
Certification Practice Statement (CPS)	A statement of practices that a Certificate Authority employs in issuing certificates.
Certificate Authority Web User Interface (GRID CA Public web UI)	A computer configured with appropriate software to support the procedures described in this CPS.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.
Certificate Revocation Identification Number(CRIN)	An encrypted message when CA issued the certificate will send user a CRIN email including the CRIN message. When the end entity requests to revoke the certificate, he or she will use the CRIN for authentication.
Public Key Certificate	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 issuer.
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. In this document, the terms "certificate user" and "relying party" are used interchangeably.
Online Certificate Status Protocol (OCSP)	A protocol for acquiring the revocation status of the certificate

Within this document the words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “OPTIONAL” are to be interpreted as in RFC 2119.

2. PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The HKU Grid CA operates a secure online repository at http://ca.grid.hku.hk/.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The following information will be published in the repository operated by the HKU Grid CA:

- The HKU Grid CA root certificate (http://ca.grid.hku.hk/cacert/cacert2.pem)
- The end entity certificates issued by the HKU Grid CA
- A Certificate Revocation List (CRL) signed by the HKU Grid CA (http://ca.grid.hku.hk/crl/cacrl2.pem)
- HKU Grid CA’s signing policy
- Procedures for each type of end entity certificates enrollment
- A copy of this CP/CPS
- An official contact email address for inquiries and fault reporting
- The physical or postal contact address
- Other general information relevant to the HKU Grid CA

2.3 TIME OR FREQUENCY OF PUBLICATION

- CA certificate, CA certificate fingerprint, and client certificate information will be published in the repository as soon as they are issued.
- CRL will be published in the repository as soon as they are issued or refreshed on schedule update.

- All HKU Grid CA documents will be published in the repository as they are updated.

2.4 ACCESS CONTROLS ON REPOSITORIES

- The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.
- The HKU Grid CA does not impose any access control on the information described in section 2.2.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

Identification of certificates will be according to X.500 distinguished name.

The following table shows the attribute values used for the name of certificates issued by the HKU Grid CA.

Attributes used in certificates

Attributes	Meaning	Value
commonName	Subscriber's name	Based on application information
commonName	Host Name	Based on application information
organizationalUnitName	Name of organization Unit	Based on application information
organizationName	Name of organization	Based on application information
domainComponent	Level 2 domain component	GRID
domainComponent	Level 1 domain Component	HKU
domainComponent	Level 0 domain Component	HK

3.1.2 Need for Names to be Meaningful

- Each host certificate must be linked to a single network entity.
- The common name of the host certificate must be the FQDN of the host.
- The Subject Name in a certificate must have a reasonable association with the end entity.

3.1.3 Anonymity or Pseudonymity of Subscribers

The subscribers cannot be anonymous or pseudonymous.

3.1.4 Rules for Interpreting Various Name Forms

See section 3.1.1.

3.1.5 Uniqueness of Names

The Distinguished Name (DN) must be unique for each certificate issued by the HKU Grid CA who has to append an additional field to names to ensure uniqueness.

For a user certificate, the CN must be the full name of the subscriber and combined with subscriber's unique ID (i.e. Staff/Student/Work ID) assigned by his/her organization. CA operator will also compare the subscriber work identity card and those of the previous archived records to ensure the uniqueness of end entity certificate. For a host certificate, the CN must be functional fully qualified domain name. For OCSP responder certificate, the CN must be combined with "ocsp" and the functional fully qualified domain name, i.e. "ocsp/[FQDN]".

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The HKU Grid CA confirms the possession of private key by verification of the CSR signature.

3.2.2 Authentication of Organization Identity

The HKU Grid CA verifies the identity of organization by checking that the organization is known to be part of HKU or its related GRID projects. Other non-HKU organizations must provide valid official documents as the proof of their involvement in Grid research projects.

3.2.3 Authentication of Individual Identity

For user certificate application, the RA verifies the identity of a person by checking:

- HKU member will be identified by inspection of the staff card or student card. Inspection will take place by the RA Operator.
- Users in other organizations must be identified by in person face-to-face interview. Photo-id and valid official documents (including work ID and the proof of work) must be presented at the interview as the proof of the end entity involvement in Grid projects and RA will preserve the copy of the individual material.

For host/OCSP responder certificate application, requests must be authorized as a legal subscriber of the HKU Grid CA and RA's approval is required before issuing host certificates for a proof of the subscriber's title of the host FQDN.

3.2.4 Non-verified Subscriber Information

No Stipulation.

3.2.5 Validation of Authority

No Stipulation.

3.2.6 Criteria for Interoperation

No Stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Enrollment request is necessary if the certificate is expired.

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The subscriber can use the CRIN (Certificate Revocation Identification Number) PIN mailed to the user during the issue of the certificate or email to gridca@hku.hk signed by a valid and trusted certificate to verify his/her identity. Subscriber can contact the RA staff in person with photo-id and valid official documents. RA verify the identity of subscriber according to section 3.2.3.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

The subscriber can be the person in specific organization, described in session 1.3.4 .

4.1.2 Enrollment Process and Responsibilities

Enrollment process for user certificate as follows and more detailed descriptions are announced on HKU Grid CA public web:

- Subscriber must fill out the user certificate application form which can be downloaded from the HKU Grid CA website and transfer it to the RA.
- The subscriber can go to HKU Grid CA website and requests for CSR. The key generation happens at the client side. A new CSR serial number would be assigned for this user certificate application.
- The RA will arrange a face-to-face meeting, or an equivalent inspection with the subscriber. The subscriber must present photo, work ID, CSR serial number and proof of work during the meeting.
- The RA examines the request according to section 3.2.
- Once the subscriber is authenticated, the RA would endorse the user certificate application form. The RA will then pass the signed application form to HKU Grid CA via signed e-mail, in person or fax.
- Upon receipt of the application form, the HKU Grid CA manager will verify the RA signature in the application form and the CSR serial number. The HKU Grid CA manager may contact the RA if necessary via signed e-mail or telephone.
- Now the CA operator will issue the certificate and sends an e-mail to the subscriber regarding the way to download the certificate.

Enrollment process for Host/OCSP responder certificate as follows:

- A subscriber who requests for Host/OCSP responder certificate must have a valid user certificate at HKU Grid CA.
- Subscriber must fill out the Host/OCSP responder certificate application form which can be downloaded from the HKU Grid CA website and transfer it to the RA.
- The subscriber can go to HKU Grid CA website and requests for CSR. The key generation happens at the client side. A new CSR serial number would be assigned for this host certificate application.
- The RA will arrange a face-to-face meeting, or an equivalent inspection with the subscriber. The subscriber must present photo, work ID, CSR serial number and proof of work during the meeting.
- The RA examines the request according to section 3.2.

- The subscriber must provide evidence or proof that the host/OCSP responder certificate request is authorized by the owner of the FQDN.
- Once the subscriber is authenticated, the RA would endorse the Host/OCSP responder certificate application form. The RA will then pass the signed application form to HKU Grid CA via signed e-mail, in person or fax.
- Upon receipt of the application form, the HKU Grid CA manager will verify the RA signature in the application form and the CSR serial number. The HKU Grid CA manager may contact the RA if necessary via signed e-mail or telephone.
- Now the CA operator will issue the certificate and send an e-mail to the subscriber regarding the way to download the certificate.

Responsibilities of the subscriber:

- Provide correct information at the enrollment.
- Manage the certificate and private key safely to prevent unauthorized uses. The private key must be protected in accordance with the "Guidelines on Private Key Protection" (OID 1.2.840.113612.5.4.1.1.1.5.4).
- The pass phrase for the private key must be at least 12 characters and RSA key must be at least 2048 bits.
- For host certificate, the private keys may be stored without a passphrase, but it must be adequately protected by system methods if stored without passphrase.
- Inform the HKU Grid CA to revoke the certificate promptly if there is any actual or suspected loss, disclosure, or other compromise of the private key.
- Inform the HKU Grid CA to revoke the certificate promptly when it is not used at all.
- Do not share any user certificate.
- Connect the server certificate with only a single network entity.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

In the enrollment process, the HKU Grid CA will check:

- The information on the application form should be valid.
- If RA examined the subscriber in a face-to-face meeting, or an equivalent inspection process.

In the certificate application process, the HKU Grid CA checks if

- The certificate request is done in accordance with the process in this document especially in the section 4.1

- The certificate request subject name has correct format; and
- The key length of the certificate request meets the requirement

4.2.2 Approval or Rejection of Certificate Applications

The issuance of a certificate by the HKU Grid CA indicates a complete and final approval of the certificate application by the CA.

If any condition specified in section 4.2.1 is not satisfied, the certificate application is rejected and the HKU Grid CA notifies to the subscriber with reason of the rejection.

4.2.3 Time to Process Certificate Applications

HKU Grid CA will process certificate applications within 3 working days after receiving the RA signed certificate application form.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Upon the checking results specified in section 4.2.1 is valid, the CA operator will store the CSR in a dedicated USB flash drive and take it to the HKU Grid CA signing server, which is kept off-line as described in 6.7.

The CA operator generates (issues) certificate containing public key from the CSR with CA signature and copy it to the online public web server by the dedicated USB flash drive.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

A notification message is sent to the e-mail address of the subscriber with the instructions on how to download it from the online public web server.

The user will be able to download his/her user certificate. For this secure http (HTTPS) connection is required.

If the authentication process specified in section 4.2.1 is not successful, the certificate is not issued and an e-mail with reason will be sent to the subscriber.

4.4 CERTIFICATE ACCEPTANCE

Subscriber and host administrator can register the certificate to the certificate stores (ex: Internet Explorer or Firefox).

If the issued certificate has any problem, the subscriber should notify the HKU Grid CA that he/she has problem to accept the issued certificate with a proper reason within 7 days from issuance of the certificate.

Unaccepted certificate should be revoked and the certificate should be re-issued.

4.5 KEY PAIR AND CERTIFICATE USAGE

HKU Grid CA certificates may be used for any software for grid computing.

User certificates must not be shared between multiple people.

Host certificates must be linked to a single network entity.

The subscriber must manage his certificates and private keys securely. To protect the private key the subscriber must encrypt his private with a pass phrase. The pass phrase must not be less than 12 characters long.

4.6 CERTIFICATE RENEWAL

HKU Grid CA does not permit certificate signing request with the same key as the previous certificate.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

Generally, certificate re-key can or must take place in cases such as:

- (case 1) after a certificate is revoked for reasons of key compromise
- (case 2) after a certificate has expired and the usage period of the key pair has also expired
- (case 3) a certificate will be expired in one month

4.7.2 Who may request Certification of a New Public Key

A subscriber of HKU Grid CA can request certification of a new public key in the following conditions.

- (case 1 in session 4.7.1) : If a certificate of the subscriber is revoked for reasons of key compromise.
- (case 2 in session 4.7.1) : If a certificate has expired and the usage period of the key pair has also expired.
- (case 3 in session 4.7.1) : If a certificate is going to be expired in one month.

4.7.3. Processing Certificate Re-keying Requests

- (case 1 in session 4.7.1) : If a certificate of the subscriber is revoked for reasons of key compromise, then the compromised certificate must be revoked and the subscriber of the certificate should follow the enrollment process (section 4.1), again to get a new certificate.
- (case 2 in session 4.7.1) : If a certificate has expired and the usage period of the key pair has also expired, then the process of re-key request processing is basically the same as the enrollment process (of section 4.1).
- (case 3 in session 4.7.1) : If a certificate is going to be expired in one month.
    - The subscriber can go to HKU Grid CA website and request for rekey Certificate Signing Request (CSR) with a different key with the previous certificate.
    - The subscriber should send an e-mail to gridca@hku.hk signed by the valid user certificate issued by HKU Grid CA. In that signed e-mail, the subscriber has to mention the current certificate serial number and newly rekey CSR serial number.
    - The subscriber must follow a new enrollment process (of section 4.1) to get a new certificate if the point of time of re-key request has passed 3 years of initial ID vetting (face-to-face meeting or an equivalent inspection process).
    - If a subscriber applies to rekey his/her certificate prior to the expiration of previous certificate, HKU Grid CA should revoke the previous certificate within 1 week after issuing the new certificate but not after the expiration time of the old certificate.
    - HKU Grid CA does not permit certificate signing request with the same key as the previous certificate. The new certificate request must use a different key with the previous certificate

4.7.4. Notification of New Certificate Issuance to Subscriber

It would be same as the initial certificate issuance in the section 4.1.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

It would be same as the initial certificate issuance in the section 4.1.

4.7.6. Publication of the Re-keyed Certificate by the CA

It would be same as the initial certificate issuance in the section 4.1.

4.7.7. Notification of Certificate Issuance by the CA to other Entities

It would be same as the initial certificate issuance in the section 4.1.

4.8 Certificate Modification

HKU Grid CA does not support certificate modification.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

HKU Grid CA can revoke the certificate and inform the subscriber if a certificate is revoked.

Subscriber must request his/her certificate revocation within 1 working day when security problems are suspected, including the following:

- 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 which could induce a critical security hole.
- The subscriber leaves his/her organization.
- In case of host certificates, the corresponding host is retired.

4.9.2. Who can Request Revocation

HKU Grid CA will accept a revocation request made by

- The certificate subscriber
- HKU Grid CA/RA
- Any other entity presenting evidence of circumstances that the criteria described in section 4.2.1 has been violated.
- Any entities presenting evidence of the compromise of associated private key.

4.9.3. Procedure for Revocation Request

- Certificate revocation request must be sent in following ways:
    - Use the CRIN (Certificate Revocation Identification Number) PIN and fill the online certificate revocation request.

  - Send the revocation request email to gridca@hku.hk signed by a valid and trusted certificate to verify his/her identity.
  - Contact the RA staff in person with photo-id and valid official documents.
- The subscriber must send a revocation request to HKU Grid CA/RA within 1 working day once a security problem is suspected.
- Then RA will forward revocation request to HKU Grid CA.
- HKU Grid CA will revoke the certificate and update the signed CRL in HKU Grid CA website. A revocation notification is sent to the subscriber through the subscriber's E-mail.

The requesting entity must specify the reason for the revocation request and provide evidence of circumstances as described in section 4.9.1.

4.9.4. Revocation Request Grace Period

HKU Grid CA will process revocation as soon as it receives the revocation request and the request is approved.

The revocation information will be published to the online repository.

During the revocation, a revocation notification is sent to the subscriber's email.

4.9.5. Time within which CA must Process the Revocation Request

The CA should process the certificate revocation request within 1 working day while receiving the request.

4.9.6. Revocation Checking Requirement for Relying Parties

No stipulation.

4.9.7. CRL Issuance Frequency (if applicable)

The lifetime of the CRL is 30 days.

A new CRL is issued immediately after any certificate revocation or at least 7 days before CRL expiration.

4.9.8. Maximum Latency for CRLs (if applicable)

CRLs must be published in the repository once it is generated.

4.9.9. On-line Revocation Status Checking Availability

HKU Grid CA system provides certificate validity information by CRL or OCSP responder.

4.9.10. On-line Revocation Checking Requirements

Prior to every usage of the certificate, its validity should be checked via CRL or OCSP responder.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Rekey Compromise

No stipulation.

4.9.13. Circumstances for Suspension

HKU Grid CA system does not support certificate suspension.

4.9.14. Who can Request Suspension

HKU Grid CA system does not support certificate suspension.

4.9.15. Procedure for Suspension Request

HKU Grid CA system does not support certificate suspension.

4.9.16. Limits on Suspension Period

HKU Grid CA system does not support certificate suspension.

4.10 CERTIFICATE STATUS SERVICES

An Online Certificate Status Protocol service is available in repository given in section 2.1.

4.11 END OF SUBSCRIPTION

If a subscriber of HKU Grid CA end the subscription to the CA services:

- The subscriber must not use any certificate issued from HKU Grid CA.
- HKU Grid CA must revoke all certificates issued for the subscriber.

4.12 KEY ESCROW AND RECOVERY

No stipulation.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 Site Location and Construction

The HKU Grid CA operates in the computer server room in HKU Information Technology Services. The access to the computer server room is restricted to authorized people.

5.1.2 Physical Access

The HKU Grid CA machines (both the signing server and the web server) are:

- Running on dedicated machines.
- Located in a secure environment where access is controlled.

Physical access to the hardware is restricted to personnel authorized to enter the computer room. Physical access to the CA machines is restricted to CA operators instructed by HKU Grid CA manager.

All events about the access to the CA machines MUST be recorded in the paper sheets prepared by security officers. The events include the names of CA operators, date and time of entering/leaving the room, and the purpose of the access to the room.

5.1.3 Power and Air Conditioning

The electric power to the HKU Grid CA machines (both the signing server and the web server) are protected by a UPS system and the building has a special air conditioning system

5.1.4 Water Exposures

The hardware is located in a zone not subject to floods.

5.1.5 Fire Prevention and Protection

The building has a fire alarm system.

5.1.6 Media Storage

Two copies of the CA private key backups are kept, one in paper format (inside a sealed envelope) and another one in CD-R format. The CA servers' backup copies are stored at removable storage media. All the copies of CA private key backups and server backups will be stored in the locked cabinet located at another room or building where access control is restricted.

5.1.7 Waste Disposal

HKU Grid CA shall ensure that all media containing sensitive information is sanitized, to remove information such that data recovery is not possible, or destroyed before release for disposal. CA personnel shall account for the destruction of sensitive information.

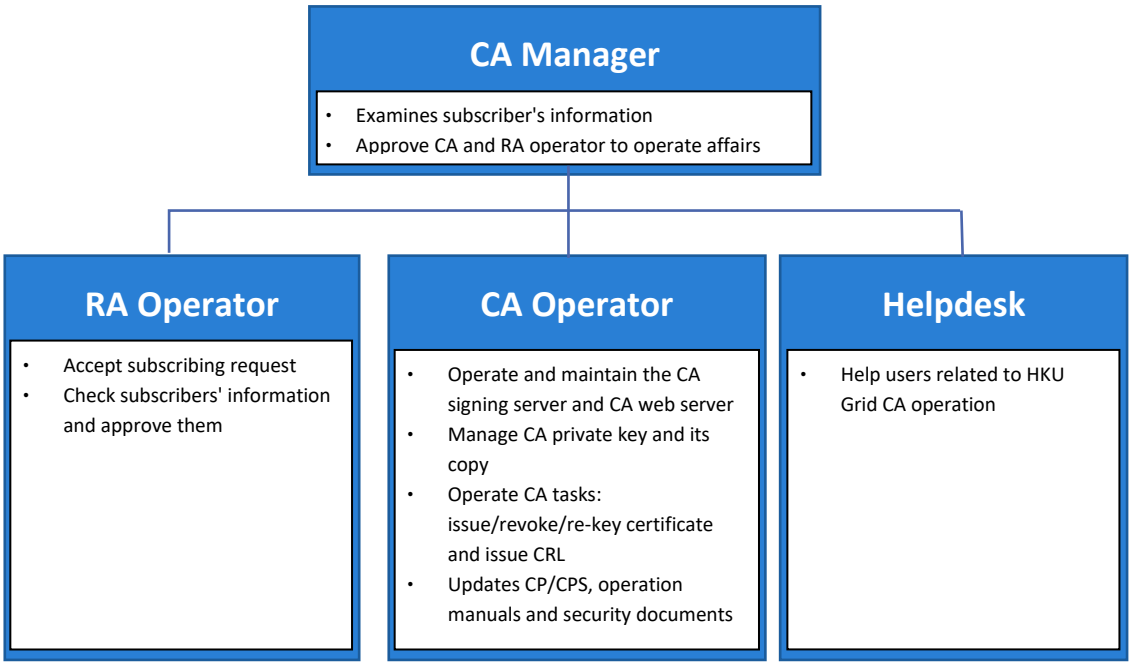
5.1.8 Off-site Backup

No stipulation.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The following figure shows the operating organization of HKU Grid CA.



The following table shows the operating roles and functions:

Role	**Function**
CA Manager	Examines subscriber's information Approve CA and RA operator to operate affairs
CA Operator	Operate and maintain the CA signing server and CA web server Manage CA private key and its copy Operate CA tasks: issue/revoke/re-key certificate and issue CRL Updates CP/CPS, operation manuals and security documents

RA Operator	Accept subscribing request Check subscribers' information and approve them
Subscriber	Use a certificate issued by HKU Grid CA
Host Administrator	The administrator of a host using a certificate issued by HKU Grid CA
Help Desk	Help users related to HKU Grid CA operation

5.2.2 Number of persons required per task

The number of staff required for each of the tasks is defined in section 5.2.1 and the number of persons for each task is described in the following:

- CA Manager: 2
- CA Operators: 2
- RA Operator: 1

All the CA/RA staffs can be act as a help desk staff.

5.2.3 Identification and authentication for each role

The HKU Grid CA system (both the signing server and the web server) will identify and authenticate the operators when the staff operates the system.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 PERSONNEL CONTROLS

Access to servers and applications is limited to the HKU Grid CA staff. No other personnel is authorized to access HKU Grid CA facilities without the physical presence of CA personnel.

5.3.1 Background, qualifications, experience, and clearance requirements

The CA shall ensure that all staff performing CA and RA functions possess the necessary knowledge, experience and qualifications to perform their duties.

5.3.2 Background check procedures

CA personnel must be a formal member of HKU Information Technology Services.

5.3.3 Training requirements

Internal training is given to CA/RA operators.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

The relevant procedural manuals required for operation of the HKU Grid CA will be provided to the staff according to their roles.

5.4 AUDIT LOGGING PROCEDURES

The HKU Grid CA and RA will retain records as much as possible so that HKU 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. The HKU Grid CA performs operational assessment of CA/RA staff at least once per year.

5.4.1 Types of events recorded

- Certification requests
- Revocation requests
- Issued certificates
- Issued CRLs
- Shutdown/boot/reboot/login/logout/sudo logs of the CA machines (both the signing server and the web server)
- Other logs archived by operating system of the CA machines (both the signing server and the web server)

5.4.2 Frequency of processing log

CA personnel will record each type of log at least once every month.

5.4.3 Retention period for audit log

The minimum retention period is 3 years.

5.4.4 Protection of audit log

The HKU Grid CA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 Audit log backup procedures

The HKU Grid CA shall back up or copy all audit logs and audit summaries.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

CA/RA records archival

- CA/RA records all the types of events listed in section 5.4.1 are archived.
- E-mail sent to/from HKU Grid CA messages will be archived as well.
- CA private keys must be stored in the safe place where access control is restricted.

RA's records all the types of events regarding user registration, certificate/revocation request including:

- date of meeting with a subscriber
- evidence of identity of a subscriber
- E-mail messages sent to/from the RA's email address.

5.5.2 Retention period for archive

Archived data will be stored for 3 years.

5.5.3 Protection of archive

Archived data with digital form will be stored in a secure operation system or periodically backup to the removable backup media. Archived data with the manual will be protected in the safe place where access control is restricted.

5.5.4 Archive backup procedures

See section 5.5.3.

5.5.5 Requirements for time-stamping of records

Archived data stored in electronic form will be time stamped.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 KEY CHANGEOVER

The HKU Grid CA root certificate has a validity of 20 years. On the other hand, the validity of client certificate, service or host certificate is only 1 year.

To avoid interruption of validity of all subordinate keys, the new CA key is generated 1 year before the old one lost validity. From that point onwards, new certificates are signed with the new CA key. The new CA public key is posted in the online repository.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If the HKU Grid CA hardware, software or data are corrupted, damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be re-established using backup hardware, software or data as quickly as possible.

If the private key of the HKU Grid CA is, or is suspected to be, compromised, the HKU Grid CA shall:

- Make all reasonable effort to inform subscribers, RAs and relying parties
- Revoke all issued certificates

- Terminate distribution services for certificates and CRLs issued using the compromised key.
- Generate a new CA key pair and certificate and make the latter available in the public repository.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If hardware, software and data are corrupted, the system must be recovered as soon as possible.

5.7.3 Entity Private Key Compromise Procedures

If an entity private key is compromised or suspected to be compromised, the entity or its administrator must request a revocation of the certificate and make all reasonable efforts to inform any known relying parties.

5.7.4 Business Continuity Capabilities After a Disaster

No stipulation.

5.8 CA OR RA TERMINATION

Before the HKU Grid CA terminates its services, the HKU Grid CA shall:

- inform APGrid PMA through APGrid PMA mailing list
- make all reasonable efforts to inform subscribers and cross-certifying CAs
- make knowledge of its termination widely available
- cease issuing certificates and CRLs
- destroy all copies of private keys

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

A CA key pair for the HKU Grid CA is generated by the HKU Grid CA staff on the CA signing server which is completely offline and not connected to any kind of network. The underlying software package used is OpenSSL. The algorithm used is SHA256 with RSA.

Each end entity MUST generate its own cryptographic keys locally by their application during the requesting process. The HKU Grid CA does not generate end entity private keys.

6.1.2 Private key delivery to entity

The end entity's private key is generated by the subscriber himself or herself. The HKU Grid CA never has access to the end entity private key.

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to users

The CA certificate is available from HKU Grid CA public repository.

6.1.5 Key sizes

The end entity key of length less than 2048 bits will not be signed. The CA's key pair length is 4096 bits.

6.1.6 Public key parameters generation

No stipulation.

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

HKU Grid CA private key is the only key used for signing CRLs and Certificates for end entity certificates.

6.2 PRIVATE KEY PROTECTION

6.2.1 Cryptographic module standards and controls

The HKU Grid CA does not use any hardware security module.

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

This CA does not yet support private key(n out of m) multi-person control. But the HKU Grid CA implements multi-person control for the access to the CA server as described in this document. The passphrase encrypting the CA private key is kept by the CA operator (2 persons). No other person knows the passphrase.

6.2.3 Private key escrow

The HKU Grid CA keys are not given in escrow. The HKU Grid CA is not available for accepting escrow copies of keys of other parties.

6.2.4 Private key backup

Two copies of the CA private key backups are kept, one in paper format (inside a sealed envelope) and another one in CD-R format. The pass-phrase of the CA private key is also kept in paper format inside another sealed envelope. All the CA private key backups and its pass-phase are stored in the locked cabinet, which is located at another room or building where access control is restricted.

6.2.5 Private key archival

See section 5.5.

6.2.6 Private Key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

See section 6.4.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public key archival

The HKU Grid CA shall retain all public key certificates it generates.

6.3.2 Certificate operational periods and key pair usage periods

The validity of each user/host certificate and key pair is 1 year.

The validity of each OCSP responder certificate and key pair is 1 year.

The validity of CA certificate and key pair is 20 years.

6.4 ACTIVATION DATA

HKU Grid CA root private key is protected by a passphrase of a minimum 15 characters. This pass phrase is only known by CA operator.

The pass phrase is backup in a sealed envelope kept in a safe place where access is controlled as mentioned in section 6.2.4.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The HKU Grid CA server includes the following:

- Operating systems are maintained at a high level of security by applying all recommended and applicable security patches;
- All related CA machines are used for dedicated purpose.

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 signing machine is kept off-line.

The CA web server machine is protected by a firewall, and it is a dedicated machine and only required services run on the server.

Appropriate software upgrade/patch of the CA web server is performed every 6 month or immediately if it is required.

The data exchange between CA signing machine and CA web server is operated manually in a secured way as mentioned in section 4.3.1. All the operations would be accomplished in the server room with restricted access.

6.8 TIME-STAMPING

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version number(s)

X.509 v3

7.1.2 Certificate extensions

The following extensions are set in the CA self-signed certificate:

- X509v3 Basic Constraints: Critical, CA:TRUE
- X509v3 Key Usage: Critical, Certificate Sign (keyCertSign), CRL Sign(cRLSign)
- X509v3 Subject Key Identifier: [the unique Key ID]
- X509v3 Authority Key Identifier: keyid
- X509v3 Issuer Alternative Name: email: gridca@hku.hk
- X509v3 Subject Alternative Name: email: gridca@hku.hk

The following extensions are set in user certificates:

- X509v3 Basic Constraints: Critical, CA:FALSE
- X509v3 Key Usage: Critical, Digital Signature (digitalSignature), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
- X509v3 Extended Key Usage: clientAuth
- X509v3 Subject Key Identifier: [the unique Key ID]
- X509v3 Authority Key Identifier: keyid
- X509v3 Issuer Alternative Name: email: gridca@hku.hk
- X509v3 Subject Alternative Name: email: [Subscriber Email address]
- X509v3 CRL Distribution Points URI: http://ca.grid.hku.hk/crl/cacrl2.der
- X509v3 Authority Information Access CA Issuers: http://ca.grid.hku.hk/pki/pub/cacert/cacert2.crt
- X509v3 Authority Information Access OCSP URI: http://ca.grid.hku.hk:2560/
- X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.30850.2.2.40000.2.1.3.0 Policy:1.2.840.113612.5.2.2.1

The following extensions are set in host certificates:

- X509v3 Basic Constraints: Critical, CA:FALSE
- X509v3 Key Usage: Critical, Digital Signature (digitalSignature), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
- X509v3 Extended Key Usage: serverAuth, clientAuth
- X509v3 Subject Key Identifier: [the unique Key ID]
- X509v3 Authority Key Identifier: keyid
- X509v3 Issuer Alternative Name: email: gridca@hku.hk
- X509v3 Subject Alternative Name: DNS: [FQDN of the host]
- X509v3 CRL Distribution Points URI: http://ca.grid.hku.hk/crl/cacrl2.der
- X509v3 Authority Information Access CA Issuers: http://ca.grid.hku.hk/pki/pub/cacert/cacert2.crt
- X509v3 Authority Information Access OCSP URI: http://ca.grid.hku.hk:2560/
- X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.30850.2.2.40000.2.1.3.0 Policy:1.2.840.113612.5.2.2.1

The following extensions are set in OCSP responder certificates:

- X509v3 Basic Constraints: Critical, CA:FALSE
- X509v3 Key Usage: Critical, Digital Signature (digitalSignature), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
- X509v3 Extended Key Usage: OCSPResponder
- X509v3 Subject Key Identifier: [the unique Key ID]
- X509v3 Authority Key Identifier: keyid
- X509v3 Issuer Alternative Name: email: gridca@hku.hk
- X509v3 Subject Alternative Name: DNS: [FQDN of the host]
- X509v3 CRL Distribution Points URI: http://ca.grid.hku.hk/crl/cacrl2.der
- X509v3 Authority Information Access CA Issuers: http://ca.grid.hku.hk/pki/pub/cacert/cacert2.crt
- X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.30850.2.2.40000.2.1.3.0 Policy:1.2.840.113612.5.2.2.1

7.1.3 Algorithm object identifiers

Signature Algorithm: sha256WithRSAEncryption(4096 bits).

7.1.4 Name forms

Issuer:
DC=HK, DC=HKU, DC=GRID, CN=HKU Grid CA 2

User certificates DN:
DC=HK, DC=HKU, DC=GRID, O=<Applicants Organization>, OU=<Applicants OrganizationUnit>, CN=<Applicants Name> (Unique ID)

Host certificates DN:
DC=HK, DC=HKU, DC=GRID, O=<Applicants Organization>, OU=<Applicants OrganizationUnit>, CN=<FQDN of host>

OCSP responder certificates DN:

DC=HK, DC=HKU, DC=GRID, O=<Applicants Organization>, OU=<Applicants OrganizationUnit>, CN=ocsp/<FQDN of host>

7.1.5 Name constraints

The round brackets symbols: `**(**' and `**)**' and the at sign '@' are not allowed for use as the "Applicants Name" for user certificate.

7.1.6 Certificate policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version number(s)

X.509 v2

7.2.2 CRL and CRL entry extensions

Signature Algorithm: sha256WithRSAEncryption

7.3 OCSP PROFILE

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1 FREQUENCY OF ENTITY COMPLIANCE ASSESSMENT

The HKU Grid CA will accept external Compliance Audit. All the CA archive records must be made available to external auditors. In addition, the HKU Grid CA performs operational self-assessment of CA/RA staff at least once per year.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The HKU Grid CA can be audited by the APGrid PMA.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The HKU Grid CA can be audited by the APGrid PMA.

8.4 TOPICS COVERED BY ASSESSMENT

The audit will focus on whether the HKU Grid CA certification duties are compliant to this CP/CPS. The HKU Grid CA is expected to operate according to the minimum CA requirements specified by the APGrid PMA.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The HKU Grid PMA has the responsibility for improving the deficiency. When the HKU Grid CA receives an audit report from the auditor, an improving report including timetable will be sent to the auditor.

8.6 COMMUNICATIONS OF RESULTS

The result of the audit will be made available to APGrid PMA in which the HKU Grid CA participates. It may make the results of the audit publicly available. The decision will be made by the HKU Grid PMA in case-by-case basis.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

No fees will be charged for any service provided by the HKU Grid CA.

9.2 FINANCIAL RESPONSIBILITY

No financial responsibility with respect to the use or management of any issued certificate is accepted.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of confidential information

Except explicit information specified in section 2.2, all other information will be treated as confidential. Confidential information will not be provided to any other people. Confidential information including personal registration information, documents and electronic media will be stored securely by a person in charge as a security officer.

9.3.2 Information not within the scope of confidential information

Data contained in CRLs and the subscriber's certificate shall not be considered confidential and will be published in a publicly accessible location.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 PRIVACY OF PERSONAL INFORMATION

Subscribers shall supply this information in enrollment form:

- Full Name
- Organization Name & Organization Unit Name
- Position
- Email, Telephone
- Photo, WorkID, & other valid official documents

HKU Grid CA would not disclose this information to other external parties except those specified in section 9.3.2

9.5 INTELLECTUAL PROPERTY RIGHTS

All certificate related data issued by HKU Grid CA is not under any copyright or intellectual property protection.

9.6 REPRESENTATIONS AND WARRANTIES

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

No stipulation.

9.8 LIMITATIONS OF LIABILITY

The HKU Grid CA has liability:

- To perform practices on the procedures according to the practices described in this document to validate identity. No other liability, implicit or explicit, is accepted. HKU Grid CA and its agents make no guarantee about the security or suitability of a service that is identified by a HKU Grid certificate.
- The certification service is run with a reasonable level of security, but it is provided on a best-effort basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.
- HKU Grid CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.
- There will be no financial liability with respect to use or management of any issued certificate.

HKU Grid CA provides its certification services on a best effort basis only and provides no warranties, express or implied, including in respect of security and confidentiality, and of fitness for a particular purpose. ITS accepts no liability for or in connection with the certification services and the parties using or relying on them shall hold ITS free and harmless from liability resulting from such use or reliance.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP/CPS is valid and enforceable from the time of accreditation by APGrid PMA.

9.10.2 Termination

This CP/CPS terminates in the following cases:

- CA certificate expires
- CA terminates its service
- A new version of CP/CPS is accredited

9.10.3 Effect of termination and survival

No stipulation.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12 AMENDMENTS

- This document and any older versions are available in repository given in section 2.1.
- Revision is made by HKU Grid PMA and approved by APGrid PMA.
- All major changes related to policy, technology or security must be approved by APGrid PMA.
- Minor changes related to editorial problems can be made without approved by APGrid PMA.
- New OID will be assigned to major changes and will not be assigned to minor changes.
- All the changes to this document must be declared in repository.
- Users will not be warned in advance of changes to this document. RA would be informed of the changes via E-mail.

9.13 DISPUTE RESOLUTION PROCEDURES

No stipulation.

9.14 GOVERNING LAW

Interpretation of this policy is according to the laws of the Hong Kong Special Administrative Region of the People's Republic of China.

9.15 COMPLIANCE WITH APPLICABLE LAW

No stipulation.

9.16 MISCELLANEOUS PROVISIONS

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10. REFERENCE

RFC 3647 - https://www.ietf.org/rfc/rfc3647.txt

Guidelines on Private Key Protection

RFC 2119 - https://www.ietf.org/rfc/rfc2119.txt