Certificate Policy

for the Chunghwa Telecom

ecommerce Public Key Infrastructure

Version 1.0

Chunghwa Telecom Co., Ltd.

October 2004

Table of Contents

1. Introduction

Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) is established to provide complete electronic certificate service in conjunction with the electronic policy and improvement of electronic commerce infrastructure of Chunghwa Telecom Co., Ltd. (hereinafter referred to as Chunghwa Telecom.)

The infrastructure follows ITU-T X.509 standard to set up the Hierarchy public key infrastructure including public key infrastructure Trust Anchor－Chunghwa Telecom Root Certification Authority(ePKI Root Certification Authority (eCA) and the Subordinate Certification Authority (CA) formed by Chunghwa Telecom. The ePKI issued certificate can be used in various applications of e-commerce to provide more secure, reliable and convenient internet service.

This Certificate Policy (CP) is a policy document based on the Electronic Signature Law and relevant international standards for the various ePKI CA to formulate their own CPS. The CP defines five Assurance Levels, namely, Level 1, Level 2, Level 3, Level 4 and the Test level, the higher the level the greater the assurance. In accordance with X.509 standard, Assurance Level must be represented by CP Object Identifier (CP OID) and such CP OID will be recorded in the certification CP (certificate Policies) extensions.

Assurance Level refers to the Relying Party’s extent of trust as in the following items:

(1) Certification Authority issued certificate can be divided into following two circumstances. If the certificate is issued for the end entity (refer to section 1.3.7) the CP OID represents what assurance level is used for identity

authentication and issuance at application of certificate; if the certificate is issued for CA then the CA certificate can possibly contain more than one CP OID and shows that CA can issue certificate to the end entity with the assurance level matching the CP OID.

(2) Relevant operation procedures for CA related systems to issue and manage certificate and to deliver the private key.

(3) Whether the subscriber or Subject in certificate data can effectively control its private key, for example, the subscriber uses software or hardware to store his/her private key.

The Public Key Infrastructure CA shall introduce appropriate CP OID for interoperability between the various Public Key Infrastructure CA and foster trans-territory operation with domestic and overseas PKI. The five assurance levels formulated by the CP can only be applied to this PKI management and interoperability while other PKI permits using the PKI CP OID in policy mapping with approved equivalent policies.

The CP formulated items and provisions are based on relevant laws and regulations and the term CA refers to all CA of this Public Key Infrastructure. Based on the principle of mutual benefits between domestic and overseas PKI, eCA with approval by Chunghwa Telecom can carry out cross-certificate with this Public Key Infrastructure CA. Any problems caused by introducing this CP by other CA other than this PKI shall be accountable by the concerned CA.

1.1 Overview

1.1.1 Certificate Policy

Certificate Policy is a guideline of the internet certificate information technology. This PKI has registered CP OID for five assurance levels so that at issuance by CA of a specific purpose certificate the assurance level can be indicated and CA can directly use the registered CP OID so that the relying parties can inspect, via the CP OID, whether the CA issued certificate is applicable and correct.

eCA certificate is a self-signed certificate and the relying source of PKI and the relying parties should directly rely on the eCA certificate. In accordance with international standards and rule, eCA certificate does not identify CP OID, therefore eCA calls for high assurance and must use level 4 assurance to operate.

1.1.2 Relationship between Certificate Policy and Certification Practice Statement

The Certification Authority (CA) shall state in the CPS how to achieve the CP assurance level.

1.1.3 Certification Authority Uses Certificate Policy object identifiers

The Public Key Infrastructure CA shall abide by this CP and not formulate its own CP. The CA shall obtain permission of Chunghwa Telecom in quoting Public Key Infrastructure CP OID and is advised to

contact Chunghwa Telecom for any relevant recommendations for CP.

1.2 Certificate Policy Identification

The Certification Authority issued certificate (not including self-signed certificate) shall record its certification CP in the CP extension. The following table shows the CP OID at id-cht arc registration:

id-cht ::= {2 16 886 1}

id-cht-ePKI ::= {2 16 886 1 100}

id-cht-ePKI-certpolicy::= {id-cht-ePKI 0}

Assurance Level	OID Name	OID Value
Test level	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
Level 1	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
Level 2	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
Level 3	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}
Level 4	id-cht-ePKI-certpolicy- class4Assurance	{id-cht-ePKI-certpolicy 4}

1.3 Principal Members and their Roles

1.3.1 Policy Management Committee

Each PKI requires a Policy Management Committee to ensure its sustained and normal operation. As regards the ePKI, Chunghwa Telecom

particularly sets up the Chunghwa Telecom ecommerce Public Key Infrastructure Policy Management Committee (ePKI Policy Management Committee) to be accountable for Chunghwa Telecom's PKI management work. The organization and tasks of the Policy Management Committee is explained below: The committee sets one convener to be appointed from the deputy general manager by the general manager; one executive secretary to be concurrently acted by Chunghwa Telecom Information Director; 9 to 11 members to be formed by representatives of ePKI and their tasks are explained below:

(1) Inspect the business model of the ePKI service comprising of: Discussion about the ePKI framework and other management matters.

(2) Inspect the ePKI CP.

(3) Inspect the CPS.

(4) Accept interoperability application for cross-certificate CA and review and approve the Certificate Policy mappings between ePKI and ePKI cross-certificate CA.

(5) Ensure ePKI CP equivalent compliance among the cross-certified CA so that the interoperable mechanism can continue to operate.

(6) Inspect relevant technical standards of ePKI.

1.3.2 Chunghwa Telecom Root Certification Authority

eCA is the top level CA of ePKI and the Principal CA representing PKI. Its principal tasks are as follows:

(1)Responsible for issuance and management of the subordinate CA.

(2)Formulate Cross-Certificate Procedures for the internal and external CA of the ePKI including issuing and managing the first level subordinate CA of the ePKI and other Public Key Infrastructure CA certification.

(3)Publish the issued certificate and Certification Authority Revocation List (CARL) in the Repository and ensure latter's normal operation. eCA shall stipulate cross-certificate procedures with CA in the CPS.

1.3.3 Subordinate Certification Authority

Subordinate CA is another type of CA in PKI principally responsible for issuing and managing certificate of end entities and if needed can also follow the hierarchical PKI structure with the first level subordinate CA issuing certificate to the second level subordinate CA, or the second level CA issuing certificate for the third level subordinate CA, and so on and so forth and build a multilevel PKI. However, the subordinate CA cannot carry out cross-certificate with CA outside the ePKI.

Establishment of subordinate CA shall follow relevant CP regulations, set up contact window to be responsible for interoperable work between eCA and its subordinate CA.

1.3.4 Registration Authority

Registration Authority (RA) is principally responsible for collecting and verifying subscriber identity, attributes, contact and relevant information to facilitate CA certificate issuance and management operation.

eCA acts the RA role by itself and executes RA work in accordance with the CPS approved by the Policy Management Committee. The subordinate CA can set up its own RA and stipulate its work in the CPS.

1.3.5 Repository

The repository provides information inquiry and download service for the various CA issued certificate, CRL and certificate status and publish relevant information for the CP and CPS certificate issuance and management operation.

The repository can be operated by the CA or other authorities but one CA does not necessarily have only one repository but shall have at least one principal repository for external service. The CA shall highlight its website in the CPS and ensure the repository's usability, appropriate access control and data completeness.

1.3.6 Other Related Members

The CA can select other relying service authority as a partner for coordinated operation such as the Audit Authority, Attribute Authority, Time Stamp Authority, Data Archiving Service and Card Management Center and stipulate in the CPS the mutual interoperable mechanism and reciprocal rights and obligations to ensure that the CA service is effective and reliable.

1.3.7 End Entities

End Entities (EE) comprise of following two entities in the ePKI:

(1)Private key owner responsible for storage and application certificate.

(2)A third party relying on the Public Key Infrastructure CA issued certificate (not the private key owner and not the CA either.)

1.3.7.1 Subscriber

To the organization and the entity, the subscriber refers to the recorded name of the certificate subject and owns the corresponding private key entity of the certificate public key. The subscriber should correctly use the certificate according to the certificate recorded CP. Moreover, as regards property type (for instance, Application Process and hardware device), the certificate subscriber is the entity or organization who applies for certificate because of disability of property itself.

In ePKI the upper CA would issue certificate for the subordinate CA but we do not call the subordinate CA as the subscriber in CP.

1.3.7.2 Relying Parties

Relying Parties refer to the certificate subject name and certain public key linked entity that trusts the certificate. Relying parties shall inspect the validity of the received certificate in accordance with the CA certificate status information.

Relying parties can use certificate to verify the completeness of the digital signature message, ensure the identity of the person who sends the message and builds a secret communication channel with the subscriber. At the same time, relying parties can also use the certificate message (such as the CP OID) to inspect whether it is the appropriate timing for using certificate.

1.3.8 Applicability

This CP has formulated five assurance levels in line with different security requirements and for different application needs. In deciding the assurance levels for the issued certificate the CA should prudently evaluate the various risks, environmental potential crisis, possible vulnerabilities, certificate usage and the importance of application within the application scope to select the assurance level for security need and carry on CA operation and issue and manage certification.

1.3.8.1 Certification Applicability

The CP has no mandatory stipulations on the assurance level's certification applicability and does not restrict use of assurance level for community groups but would like to explain the recommended applicability:

Assurance Level	Applicability
Test level	For Test only and does not carry any legal responsibility pursuant to the delivered data.
Level 1	Rudimentary assurance level appropriate for applications in internet environment with very low threat of vicious tempering or use to identify subscriber entity name and assure the completeness of the signed document when a higher assurance level is not available. It is not suitable for using in online trading that needs certification.

Level 2	Basic assurance level appropriate for applications in information in internet environment that could be tempered but with no vicious tempering (information could be intercepted but the possibility is not high) and is not suitable for signature of important documents.
Level 3	Medium assurance level appropriate for applications in internet environment with comparatively higher risk than level 2 that the vicious user can intercept or temper information and the delivered information could include online transaction of money.
Level 4	High assurance level appropriate for applications in internet environment with very high risk of potential threat or a very high restoration price after information is being tempered, and the delivered information includes high value online transaction or extremely confidential documents.

1.3.8.2 Certification Usage Restrictions

End Entities should select the appropriate assurance level certification in accordance with the necessary security requirements of the application system.

In using the private key the subscriber should select a secure and reliable computer environment and application system to avoid theft of the private key and impair benefits.

The application system shall follow stipulations in section 6.1.9 key

usage purpose and appropriately use the key and process the critical certificate extensions.

1.3.8.3 Prohibited Usage Scope for Certification

The Public Key Infrastructure CA issued certificate is prohibited for using in the following scope:

(1) Crime.

(2) Military order war intelligence and nuclear and biochemical weapons control.

(3) Nuclear-powered equipment

(4) Aviation flying and control systems.

1.4 Contact Method

1.4.1 Certificate Policy Formulation and Management Authority

Chunghwa Telecom Co., Ltd.

1.4.2 Contact Information

Please contact this Company for recommendations to the CP. Go to: http://epki.com.tw

1.4.3 CPS Review

CA should first check whether CPS conforms to the relevant CP regulations and forward to the Policy Management Committee for review

and approval. After approval CA can formally use the ePKI CP.

According to stipulations of the R.O.C. Electronic Signature Law, CA formulated CPS shall be approved by the competent authority of the Ministry of Economic Affairs before starting to provide certificate issuance service.

Chunghwa Telecom has the right to audit whether CA complies with CP (as stipulated in section 2.7) CA should also regularly carry out self-auditing to verify that operation is being carried out by the CP assurance level.

2 General Provisions

2.1 Responsibility and Obligations

2.1.1 Responsibility of Certification Authority

The responsibility of the CA is as follows:

(1) Issue and publish certificates.

(2) Execute the authentication procedures stipulated in Chapter 3.

(3) Publish the revoked and suspended certificates.

(4) Issue and publish CARL or CRL. (No stipulations for CA operated with test assurance level.)

(5) Provide relevant control in accordance with stipulations in Chapters 4 and 6.

(6) Publish in CPS and explain its responsibility for the subscriber and the relying parties.

(7) Protect the private key in accordance with stipulations in Chapters 4, 5 and 6.

(8) The CA private key can only be used in certification issuance, CRL, signature or relevant information required for issuing certificate in accordance with the different certificate assurance levels.

(9) Follow the CP in formulation of CPS.

2.1.2 Responsibility of Registration Authority

Responsibility of the RA is as follows: (No stipulations for CA operated with test assurance level.)

(1) Provide relevant control in accordance with Chapters 4, 5 and 6.

(2) Carry out identification and authentication of certificate application in accordance with stipulations in Chapter 3.

(3) Notify subscriber and relying party the responsibility and obligations of CA and RA.

(4) Notify the subscriber and the relying party for compliance with relevant CP stipulations in using or accepting CA issued certificate.

(5) Protect the private key in accordance with stipulations in Chapters 4, 5 and 6.

(6) The private key shall be used in accordance with stipulations in section 6.1.9 and shall not be used in operations outside of certification registration without CA permission.

2.1.3 Subscriber Obligations

In accepting the CA issued certificate the subscriber has following obligations:

(1) Abide by stipulated procedures in Chapters 3 and 4.

(2) Correctly use certificate.

(3) Properly store and use the private key.(No stipulations for certificate

issued with the test assurance level.)

(4) Notify the CA immediately when the private key is being decrypted. (No stipulations for certificate issued with the test assurance level.)

2.1.4 Obligations of Relying Parties

In using CA issued certificate the relying parties has following obligations:

(1) Familiar with the applicable scope and assurance level.

(2) Use certificate in accordance with the applicable scope.

(3) Correctly inspect the digital signature.

(4) Correctly inspect the CARL and CRL.(No stipulations for certificate with the test assurance level.)

2.1.5 Obligations of Repository Service

The CA repository service has following obligations:

(1) Regularly publish the issued certificate.

(2) Regularly publish the revoked and suspended certificate information.

(3) Publish the latest CP and CPS information.

(4) Access control of the repository shall abide by stipulations in section 2.6.3.

2.2 Legal Responsibility

2.2.1 Responsibility of the Certification Authority

2.2.1.1 Guarantee Scope and Restrictive Conditions

If CA used any CP formulated assurance level OID in the issued certificate represents CA guarantees the content information of the issued certificate has abided by CP stipulations. Except that CA genuinely abided by CP stipulations, otherwise the issued certificate shall not use any CP stipulated assurance level CP OID.

2.2.1.2 Disclaimers and Limitations

CA should carry Disclaimers and Limitations in the CPS to exclude mistakes for CA responsibility. But CA shall not exclude consequences arising from self-negligence.

2.2.1.3 Upper Limit of Responsibility

CA shall state in the CPS the upper limit of responsibility.

2.2.1.4 Other Exemption Provisions

Force Majeuvre and other reasons not attributable to CA including disasters, accidents, incidents, specific events that caused damage; CA shall state in the CPS other exemption provisions but shall not exclude mistakes arising from self-negligence.

2.2.2 Responsibility of Certification Authority

CA shall assume all responsibilities from work because of RA acting on

behalf of CA and the responsibility of RA depends on its rights and obligations of CA. CA shall state the responsibility of RA in the CPS or contract with RA or agreement.

2.2.2.1 Guarantee Scope and Limitations

No stipulations.

2.2.2.2 Disclaimers and Limitations

No stipulations.

2.2.2.3 Upper Limit of Responsibility

No stipulations.

2.2.2.4 Other Exemption Provisions

No stipulations.

2.3 Financial Responsibility

2.3.1 Indemnification by Subscriber and Relying Parties

CA shall state in the CPS the indemnity responsibility of subscriber and the relying parties.

2.3.2 Administrative Processes

The competent authority of CA decides administrative processes of CA.

2.4 Interpretation and Implementation

2.4.1 Applicable Law

The interpretation and legality of any agreement signed by CP shall abide by relevant laws and regulations.

2.4.2 Severability of Provisions, Survival, Merger and Notice

If any chapter and section in CP is incorrect or invalid, other chapters and sections remain effective and revision of CP shall follow stipulations in section 8.1.

2.4.3 Dispute Resolution Procedure

If dispute arises from interpretation of content in CP, both parties should seek consultation for consensus. If consultation fails, ask for interpretation in accordance with the dispute resolution procedure formulated by Chunghwa Telecom. CA shall state the dispute resolution procedures in the CPS.

2.5 Fee

2.5.1 Certificate Issuance and Extension Fee

No stipulations.

2.5.2 Certificate Inquiry Fee

No stipulations.

2.5.3 Certificate Revocation and Status Inquiry Fee

No stipulations.

2.5.4 Other Service Fees

No stipulations.

2.5.5 Refund Procedures

No stipulations.

2.6 Publication and Repository

2.6.1 CA Information Publication

CA should publish in a designated repository:

(1) Certificate Practice Statement (CPS).

(2) Certification Revocation List (CRL) (or provide Online Certificate Status Inquiry) including CRL issuance time and valid date and certificate termination time.

(3) Certificate of CA itself shall at least be the valid date of all certificates issued by the corresponding private key.

(4) All issued certificates (including certificate issued for other CA.)

(5) The issued CARL (such as CA issued certificate for other CA.)

(6) Privacy protection policy.

Except for foregoing information CA shall publish necessary

information that can verify digital signature.

Certification Authority CPS shall state the upper limit of temporary suspension of service time in the repository.

2.6.2 Publication Frequency

Certification Revocation List (CRL) publication frequency shall follow stipulations in section 4.4 and CP publication shall follow stipulations in Chapter 8.

2.6.3 Access Control

(1) No access control for acquisition of CP and CA.

(2) Certification Authority (CA) decides by its own whether certificate requires access control.

CA should protect information in the repository to avoid vicious public dissemination or tempering. Public key certificate and certificate status information should be obtained openly from the internet.

2.6.4 Repository

In accordance with stipulations in section 1.3.5, the repository can be operated by the CA or other authorities and the CA CPS should carry relevant information in the repository.

2.7 Auditing Method

In issuing assurance levels 2, 3 and 4 certificates the CA shall establish a compliance audit mechanism to ensure that its operation abide by CPS and CP

stipulations.

2.7.1 Auditing Frequency

CA shall accept regular auditing and in accordance with assurance levels 3 and 4 CA shall accept at least one auditing each year and in accordance with assurance level 2 CA shall at least accept auditing every other year. In accordance with the test assurance level and Level 1 operation no stipulations is made for CA.

Certification Authority (CA) shall carry out regular and irregular auditing for its subordinate CA and RA to ensure its subordinate entities follow CPS operations.

2.7.2 Auditor Identity and Qualifications

Auditors shall be independent of the CA being audited and the following entity shall take up the responsibility:

(1) A fair third party.

(2) An independent entity in the organization differing from the CA being audited.

The auditor shall provide fair and independent appraisal and its qualifications shall be approved by Chunghwa Telecom and familiar with the relevant regulations for certificate issuance and management by the CA. CA shall verify the identity of the auditor at auditing.

2.7.3 Relationship between the Auditor and the Audited Party

In accordance with stipulations in section 2.7.2 auditors shall be

independent of the CA being audited.

2.7.4 Audit Scope

The audit scope is stipulated as follows:

(1) CA follows CPS operation.

(2) CPS conforms to CP stipulations.

(3) Auditors can audit relevant operation units of CA such as the RA.

In the event CA and its subordinate CA sign cross-certificate agreement the audit scope should include whether the subordinate CA conforms to stipulations of the cross-certificate agreement.

2.7.5 Countermeasures for Audited Results

If the auditor finds out CA establishment and operation do not conform to stipulations of CP or cross-certificate agreement, it is necessary to take following actions:

(1) The auditor should record the non-conformances.

(2) The auditor should notify the competent authority of the CA about the non-conformances and if the non-conformance is serious the auditor should notify the Policy Management Committee.

In the event of nonconformance the CA should make revisions in accordance with the audit report or stipulations of the cross-certificate agreement.

2.7.6 Open Scope of Audited Results

No stipulations.

2.8 Scope of Information Confidentiality

2.8.1 Type of confidential information

(1) Any personal or organization information at certificate application is confidential and shall not be made public without subscriber permission or as required by laws and regulations.

(2) The private key and password for CA operation are confidential information and shall not be made public.

(3) Except for stipulations in section 2.7.6 the audit log shall not be made public in its entirety.

CPS shall state the type of confidential information.

2.8.2 Type of Non-confidential Information

(1) Certificate, CRL and revoked or suspended information shall not be regarded as confidential information.

(2) Except stipulated otherwise identification information or information recorded on the certificate should not be regarded as confidential information.

CPS shall state the types of non-confidential information.

2.8.3 Opening of Certificate Revocation or Temporary

Suspended Information

Certificate revocation or temporary suspended information are non-confidential and should be made public.

2.8.4 Information Release at Request of Judiciary

CPS shall formulate relevant stipulations in section 2.8.1 on confidential information for the judiciary.

2.8.5 Information Release at Request of Civil Litigation

CPS shall formulate relevant stipulations in section 2.8.1 on confidential information for civil litigation.

2.8.6 Information Release at Request of Subscriber

CPS shall formulate relevant stipulations in section 2.8.1 on confidential information for subscriber.

2.8.7 Other Situations for Information Release

In accordance with relevant laws and regulations.

2.9 Intellectual Property Rights

The CP is the intellectual property of Chunghwa Telecom and in accordance with relevant laws and regulations the CP can be reproduced or disseminated but shall guarantee it is a complete reproduction and state that the copyright is owned by Chunghwa Telecom. Collection of fee is prohibited for reproduction or dissemination and improper use or infringement on dissemination of the CP shall be pursued by Chunghwa Telecom in accordance with the law.

3 Identification and Authentication Procedures

3.1 Initial registration

3.1.1 Name forms

The PKI certificate subject name should be a distinguished name (DN) of X.500.

In certificate application the CA has the right to decide whether to accept or not Subject Alternative Name and if the CA requires to add a Subject Alternative Name in the certificate, the extension shall be indicated as a non-critical extension.

3.1.2 Need for names to be meaningful

The organizational or personal certificate subject name shall conform to the subject naming regulations of the R.O.C. relevant laws and regulations and use the official registered name.

The certificate subject name of the equipment or server shall be the name of the administrator of equipment or server software and at the same time use the Common Name for easy understanding, for instance, the module name or serial number or application procedure, etc.

3.1.3 Rule for interpretation of names

Chunghwa Telecom is responsible for setting up the rule for interpretation of names including the certificate format dissection.

3.1.4 Uniqueness of name

The certificate subject name in the ePKI shall be unique. Chunghwa Telecom is responsible for setting up relevant regulations governing the use of the X.500 Name Space by the CA to ensure the uniqueness of names; the CA shall state in the CPS how to use the X.500 Name Space, and at the same time ensure the uniqueness of the certificate subject name in naming identical names of the certificate subject.

3.1.5 Naming Dispute Resolution Procedure

The naming right should follow the naming rules of the relevant R.O.C. laws and regulations (such as the company law, the name law and the national education law, etc.) The CA shall formulate the naming dispute resolution procedures in the CPS. The CA operating in accordance with the test assurance level has no stipulations.

Chunghwa Telecom shall be the arbitration authority for ePKI naming dispute.

3.1.6 Recognition, authentication and role of trademarks

If the certificate subject name comprises of a trademark its naming shall conform to the relevant R.O.C. trademark laws and regulations.

3.1.7 Certificate for Ownership of Private Key

In certificate application the CA shall verify that the applicant owns the private key and will become a key pair with the public key on the certificate.

Different key generator shall use different methods to certify ownership of the private key. CP has following three accredited certification methods:

(1)When the CA or RA generates the key pair for subscriber:

The subscriber is not required to verify ownership of the private key but shall accept identity authentication in accordance with stipulations in sections 3.1.8, 3.1.9 and 3.1.10 to obtain the private key and the activation data, and the private key shall be delivered to the subscriber in accordance with stipulations in section 6.1.2.

(2)When a relying third party (for example the Card Issuance Center) generates key pair for the subscriber:

The CA or RA shall obtain the subscriber public key from a relying third party through the secure channel in accordance with section 6.1.3; the subscriber is not required to certify ownership of the corresponding private key but shall accept identity authentication in accordance with stipulations in sections 3.1.8, 3.1.9 and 3.1.10 and obtain the private key and activation data, and the private key shall be delivered to the subscriber in accordance with section 6.1.2.

(3)When the subscriber generates key pair by itself:

The subscriber can use the private key to generate a signature and provide the signature to the CA or RA in accordance with stipulations in section 6.1.3, and the CA or RA uses the subscriber public key to verify the signature to certify the subscriber owns the private key. CP permits using other secure methods (such as the various methods listed in RFC 2510 or RFC 2511) to certify ownership of the private key.

3.1.8 Organization Identity Authentication Procedures

Different assurance levels have different stipulations for the required number of documents, authentication procedures and necessity for application at the counter for organization identity authentication and is listed in the table below:

Assurance level	Organization Identity Authentication Procedures
Test level	No stipulations.
Level 1	(1)No written document authentication. (2)Can apply certificate if applicant has email address and authentication procedure is not required. (3)Counter application not required.
Level 2	(1)No written document authentication. (2)Subscriber submits organization information such as organization identification code (such as business license number), organization name, etc. for the CA to compare with accredited data. (3)Counter application is note required.
Level 3	Organization identity authentication is divided into following ways: (1)Chunghwa Telecom organization identity authentication Chunghwa Telecom organizations shall use official

Assurance level	Organization Identity Authentication Procedures
	document to apply for certificate and the CA or RA shall verify the existence of the organization or unit and verify the documents are genuine. (2)Civic Organization Identity Authentication Application information includes organization name, location, name of representative, etc. that can be used to identify the organization. Aside from verifying the application information and the identity of the representative are true the CA or the RA shall also verify the representative has the right to apply for certificate using the name of the organization. At application the representative shall apply in person at the CA or RA and if the representative cannot apply in person at the counter he/she shall appoint a surrogate with a written document to apply at the counter and verify the identity of the surrogate in accordance with stipulations of the third assurance level in section 3.1.9. If the civic organization has gone through foregoing identification and authentication at the counter in advance by the CA, RA or the relying authority or person of the CA (such as a notary) and left behind information of evidence for identification and authentication, then the representative is not required to apply in person at the counter and the CA or RA will verify the authentication information.

Assurance level	Organization Identity Authentication Procedures
	Furthermore, certificate application via government PKI issued third assurance level certificate signature the representative is not required to apply in person and the CA or RA will verify the digital signature of the application information. The civic organization mentioned above refers to the legal private institution, the non-legal private institution or the affiliated organization of the two organizations.
Level 4	Organization identity authentication can be divided into following two ways: (1)Chunghwa Telecom or unit identity authentication. Chunghwa Telecom or unit shall use official document to appoint verifiable individual of the CA or RA to represent the authority or unit to apply in person at the CA or RA and latter should verify the authority or unit really exists and verify the documents are true and verify the identity of the authority or unit in accordance with stipulations in section 3.1.9 using level 4 assurance level. (2)Civic organization identity authentication Application information comprises of the organization name, location and the name of the representative that can be used to identify the organization. Aside from verifying the

Assurance level	Organization Identity Authentication Procedures
	application data and the representative identity are true the CA or RA shall also verify that the representative has the right to use the organization name to apply for certificate. At application the representative shall apply in person with the CA or RA. The civic organization mentioned above refers to the private legal group, non-legal group or the affiliated organization of the above two organizations.

3.1.9 Individual Identity Authentication Procedures

As regards Individual identity authentication, different assurance levels have different stipulations in terms of the number of documents, the authentication assurance procedures and whether or not necessary to apply in person at the counter. See table below:

Assurance level	Individual Identity Authentication Procedures
Test level	No stipulations.
Level 1	(1)Written document authentication not required. (2)Applicant with email address can apply for certificate; authentication assurance procedures not required. (3)Application at counter not required.
Level 2	(1)Written document authentication not required.

Assurance level	Individual Identity Authentication Procedures
	(2)Subscriber submits personal information such as individual identification code (such as ID number), name, etc. for comparison with accredited data by CA. (3)Application at counter not required.
Level 3	(1)Verify written document: In applying for certificate subscriber shall at least present one accredited original document with attached photo (such as national ID card) for CA or RA to verify subscriber identity. If subscriber (such as non-adult) has no document with photo, government issued written document (such as the residence account book) that can prove subscriber identity can be used instead and have one adult with capability of conduct to ensure subscriber identity with written guaranty; but the identity of the adult providing written guaranty shall be verified as mentioned above. (2)Subscriber submitted individual information, for instance personal identification code (such as the ID card number), name and address (such as residence address) etc. shall be compared with the registered data of the competent authority (such as residence data) or other registered data of a relying third party accredited by the competent

Assurance level	Individual Identity Authentication Procedures
	authority. (3)Application at counter: Subscriber shall verify his/her identity in person at the CA or RA. If subscriber cannot apply in person he/she can appoint surrogate with written document for application at counter but the CA or RA shall verify the document is true (for instance verify the subscriber seal on the written document) and verify the identity of the surrogate mentioned above. If the individual has gone through the counter identification and authentication procedures in advance conforming to the foregoing stipulations with the CA, RA or the CA relying authority or individual （such as notary） and has left information as evidence for identification and authentication, then the individual is not required to apply in person but the CA or RA shall verify the information used as evidence. (4) Use natural person to apply for certificate In using the certificate signature issued by the CA of the Ministry of Interior Affairs with a third assurance level subscriber is not required to verify his/her identity in person at the CA or RA but the CA or RA shall verify the signature

Assurance level	Individual Identity Authentication Procedures
	is valid.
Level 4	(1) Verify written document: In applying for certificate subscriber shall present at least one accredited original document with photo (such as the national ID card) for the CA or RA to verify subscriber identity. (2) Subscriber submitted personal information such as personal identification code (such as ID card number), name and address etc. (such as residence address) should be compared with the registered data of the competent authority (such as residence information). (3) To apply at counter subscriber shall verify his/her identity in person at the CA or RA.

3.1.10 Component Authentication Procedure

Computer and telecommunications equipment (such as router, firewall, etc.) or software (such as Web Server) are disability in law; the organization or individual shall present certificate application by the equipment administrator; identity authentication of the organization or individual shall follow stipulations in accordance with sections 3.1.8 or 3.1.9.

3.2 Certificate Key Replacement and Extension

3.2.1 Certificate Key Replacement

When the subordinate CA replaces key pair the CA issuing certificate to its subordinate CA shall carry out identification and authentication in accordance with stipulations in section 3.1 and issue the new certificate to the subordinate CA.

If the subordinate CA subscriber requires to replace key it is necessary to conform to requirements listed in the table below:

Assurance level	Authentication requirements for subscriber certificate key replacement
Test level	Not stipulated.
Level 2	Subscriber identity can use current signature key for authentication and carry out authentication in accordance with initial registration authentication procedures in section 3.1.
Level 3	Subscriber identity can use current signature key for authentication and carry out authentication in accordance with initial registration authentication procedures in section 3.1. but if the time interval of initial registration exceeds 15 years then it is necessary to apply for initial registration in accordance with stipulations in section 3.1.
Level 3	Subscriber identity can use current signature key for authentication and carry out authentication in accordance with

Assurance level	Authentication requirements for subscriber certificate key replacement
	initial registration authentication procedures in section 3.1. but if the time interval of initial registration exceeds 9 years then it is necessary to apply for initial registration in accordance with stipulations in section 3.1.
Level 4	Subscriber identity can use current signature key for authentication and carry out authentication in accordance with initial registration authentication procedures in section 3.1. but if the time interval of initial registration exceeds 3 years then it is necessary to apply for initial registration in accordance with stipulations in section 3.1.

3.2.2 Certificate Extension

CA certificate cannot be extended and only subscriber certificate can be extended and can use the current signature key for authentication.

3.3 Certificate Revocation Key Replacement

After certificate revocation the new certificate shall be issued in accordance with stipulations in section 3.1 and subscriber shall file for initial registration procedures again.

3.4 Certificate Revocation

CA or RA shall carry out authentication of certificate revocation application and CA shall state applicant’s identity authentication in the CPS in accordance

with stipulations in section 4.4 and make sure the applicant has the right to file for certificate revocation.

Regardless of whether the private key is being decrypted or not the private key signature and the revoked certificate can be used to verify the identity of the applicant.

4 Operational Requirements

4.1 Certificate Application Procedures

CA shall state application procedures for initial registration, certificate extension, certificate key replacement, application venue or website in the CPS.

eCA can accept Chunghwa Telecom established CA to apply for certificate and become the first level subordinate CA in the ePKI and the application procedures shall be formulated by the Policy Management Committee.

The Policy Management Committee shall formulate the cross-certificate procedure for CA outside of ePKI for eCA application.

All level subordinate CA in the ePKI shall not accept other CA application to become its subordinate CA except with permission from the upper level CA.

Before eCA issues cross-certificate for CA outside of the ePKI, the Policy Management Committee and the CA should consult to decide whether to recognize the cross-certificate issued by the CA to the other CA.

4.2 Certificate Issuance Procedures

CA issued certificate shall follow stipulations in section 5.2 and in the CPS and have the appropriate personnel execute the relevant tasks of certificate issuance and the CA or RA shall notify the applicant in an appropriate way after certificate issuance. CA that operates under assurance levels 1, 2, 3 and 4 shall state in the CPS how to notify the applicant after certificate issuance.

If CA or RA does not agree to issue certificate the applicant shall be

properly notified and precisely informed the reasons for not issuing certificate. Except for reasons of identification and authentication of the applicant identity, the CA can refuse to issue certificate for other reasons. CA operating with assurance levels 1, 2, 3 and 4 shall state in the CPS the way of notification for refusing to issue certificate.

eCA shall issue a Self-Signed Certificate and after the Policy Management Committee verifies the contents are correct the certificate shall be delivered to the relying party in accordance with stipulations in section 6.1.4.

In issuing cross-certificate the eCA shall clearly indicate the Path Length Constraint in the basic Constraints extensions to ensure the interoperable path is permitted and the set value of the certificate path length constraint is set in the permitted certificate interoperable path length.

4.3 Certificate Acceptance Procedures

After issuance of certificate with assurance levels 2, 3 and 4 the CA will publish the issued certificate in the repository only after the certificate applicant has reviewed the certificate content and accepted the issued certificate. If the certificate applicant refuses to accept the issued certificate after reviewing the contents the CA shall revoke the certificate. CA that operates under assurance levels 2, 3 and 4 shall state in the CPS following items:

(1) The certificate applicant shall confirm whether to accept or reject the certificate.

(2) Before deciding to accept the certificate the applicant shall review the certificate field.

(3) Way of handling if the applicant refuses to accept the certificate.

Before accepting certificate the applicant shall review the certificate field comprising at least the certificate subject name. As regards handling of rejection of certificate by the applicant the way of handling shall be in accordance with the principle of consumer protection law and the fair trade law if fee collection or refund is involved.

Only after the Policy Management Committee confirmed the content of the eCA self-signed certificate shall be disseminated to the relying parties in accordance with stipulations in section 6.1.4.

4.4 Certificate Temporary Suspension and Revocation

Except for CA that operates under test assurance level, other CA shall provide certificate revocation service; CA shall decide whether to provide temporary certificate suspension service in accordance with certificate application scope and service quality.

CA that provides certificate revocation or temporary certificate suspension service shall stipulate in the CPS the service time for providing certificate revocation or temporary suspension application.

CA that provides certificate revocation or suspension service shall state in the CPS the service provided, the certificate revocation application procedures, the application venue or website, etc.

After revocation or suspension of certificate, the CA shall list the revoked or temporarily suspended certificate into the CARL or CRL and publish in the repository before the next scheduled publication of CARL or CRL; and the

published certificate status information shall comprise of the revoked or temporarily suspended certificate until these certificates expire or restored usage.

Regarding the expired certificate CA shall not handle the application for certificate revocation or temporary suspension nor list the revoked or temporarily suspended information into the CARL or CRL. But regarding the revoked or suspended certificate prior to expiration, CA shall list the revoked or suspended information into the CARL or CRL at least once.

4.4.1 Reasons for Revoking Certificate

Certificate shall be revoked for one of the following circumstances:

(1) If the subscriber private key has been proven or suspected to be decrypted (for instance loss of the IC card for storing subscriber private key), then the unexpired public key certificate corresponding to the private key shall be revoked.

(2) If the CA private key has proven to be decrypted then the unexpired cross-certificate issued to the CA shall be revoked.

(3) If the certificate subject information or attributes changed (for instance change of subject name, subject number or code, and the subject identity disappears because of dissolution or death) and is sufficient to affect the correctness of the certificate recorded data, then the unexpired certificate subject shall be revoked.

Except for above reasons that certificate shall be revoked, subscriber shall file application for certificate revocation within the valid period of the

certificate.

If CA or RA has proven subscriber has violated subscriber obligations stipulated in the CP or CPS, CA can directly revoke the subscriber certificate.

If CA has proven or suspected its private key has been decrypted, it can directly revoked all certificate issued by the private key.

If the upper CA has proven the subordinate CA has violated the CP or CPS, former can directly revoke the certificate of the subordinate CA.

If CA has proven its cross-certificate CA has violated CP or its own CPS, former can directly revoke the cross-certificate of the said CA.

If the Policy Management Committee has decided that the eCA self-signed certificate shall be revoked (for instance eCA private key is suspected of being decrypted), former can directly revoke its eCA self-signed certificate.

4.4.2 Certificate Revocation Applicant

In the event certificate shall be revoked or because of other circumstances stipulated in section 4.4.1, the subscriber or entity that owns the private key shall file for certificate revocation application with the CA or RA within the valid period of certificate.

In accordance with stipulations in section 4.4.1 CA can directly revoke certificate of the subscriber, the subordinate CA or cross-certificate CA.

4.4.3 Certificate Revocation Procedures

Upon receipt of certificate revocation application the CA or RA shall carry out applicant identity identification and authentication in accordance with stipulations in section 3.4 and the CPS, and if the identity identification or authentication is correct and the reasons for revocation justifiable, for instance CA key decryption shall not be selected without justifiable reasons, then the application for certificate revocation shall be approved.

If certificate revocation application or decision to directly revoke the certificate is concurred, then CA or RA shall arrange to have appropriate personnel to carry out the relevant tasks for certificate revocation in accordance with stipulations in section 5.2 and the CPS and after revocation of certificate CA or RA shall notify subscriber with the most appropriate method. CA that operates under assurance levels 1, 2, 3 and 4 shall state in the CPS how to notify the subscriber after certificate being revoked.

If certificate revocation is not concurred, CA or RA shall notify subscriber in an appropriate way the reasons for not agreeing to revoke certificate. CA that operates under assurance levels 1, 2, 3 and 4 shall state in the CPS the way of notification regarding the reasons for not agreeing to revoke the certificate.

4.4.4 Handling Period for Certificate Revocation Application

If subscriber or CA has the need to carry out certificate revocation application with CA which issued certificate shall be speedily filed, and except for assurance level 4, the various CA shall complete certificate

revocation operation within one working day after receipt of application.

4.4.5 Reasons for Temporary Suspension of Certificate

CA that provides temporary suspension of certificate service shall state in the CPS the reasons why the certificate must be or shall be temporarily suspended.

4.4.6 Applicant for Temporary Suspension of Certificate

CA that provides temporary suspension of certificate service shall state in the CPS the identity of the applicant for permission to temporarily suspend certificate.

4.4.7 Certificate Temporary Suspension Procedures

CA that provides temporary suspension of certificate shall state in the CPS the temporary suspension certificate procedures.

4.4.8 Certificate Temporary Suspension Handling Period

CA that provides certificate temporary suspension service shall state in the CPS the certificate temporary suspension handling period for subscriber application.

4.4.9 CARL and CRL Issuance Frequency

eCA shall issue CARL and the subordinate CA and cross-certificate CA shall issue CARL or CRL. Before issuing CARL or CRL it is necessary to inspect its contents, verify the information is correct, for instance, use software to scan the CARL or CRL to inspect data correctness. CARL or

CRL shall be regularly published even if the certificate status has not changed to ensure real-time status for certificate information.

Publication of certificate status information shall be completed before update of the following certificate status information, thereby to assist offline or remote operation of the application system and the certificate status information shall be stored in the local cache. CA shall improve coordination with the repository to minimize the time required from generation of certificate status information to publication in the repository and the CPS shall stipulate which is the principal repository so that subscriber can go to that repository to retrieve the latest certificate status information.

At publication of certificate status information the overdue certificate status information shall be removed from the repository. The following table shows the relevant regulations governing the issuance frequency of CARL and CRL.

Assurance level	CARL issuance frequency	CRL issuance frequency
Test level	N/A	No stipulations
Level 1	N/A	No stipulations
Level 2	N/A	At least once every 3 days
Level 3	At least once a day	At least once a day
Level 4	At least once a day	At least once a day

4.4.10 CARL and CRL Inspection Rules

Relying parties using assurance levels 2, 3 and 4 shall inquire the current CARL and CRL before using certificate to inspect the current certificate status and at the same time also to verify the CARL and CRL are true and complete. Relying parties shall consider the risk of assumption, responsibility and influence and decide by themselves the time interval for accessing the new certificate revocation information in accordance with stipulations of relevant obligations in section 2.1.4.

4.4.11 Online Certificate Status Inquiry Service

Aside from providing CARL or CRL service the CA shall also selectively provide relying parties online certificate status inquiry service. The online certificate status inquiry service provided by the CA shall conform to the IETF RFC 2560 standard and the freshness of the provided certificate status information shall at least equivalent to the update of the CARL or CRL, that is to say the certificate status response of this Update shall at least be equivalent to the this Update of the latest CARL or CRL. If subscriber uses online certificate status inquiry provided by the CA, then it is not required to obtain or handle the CARL or CRL published by the said CA. CA shall state in the CPS whether and how online certificate status inquiry service is provided.

4.4.12 Online Certificate Status Inquiry Rules

If relying parties using assurance levels 2, 3 and 4 do not inspect CARL or CRL then it is required to verify certificate status by online inquiry.

4.4.13 Other Revocation Announcements

No stipulations.

4.4.14 Other Revocation Announcement Inspection Rules

No stipulations.

4.4.15 Other Special Regulations for Key Decryption

When key is being decrypted, follow relevant stipulations in sections 4.4.1, 4.4.2 and 4.4.3 for handling.

4.5 Security Auditing Procedures

CA that operates under test assurance level without security audit function can issue other assurance level certificate for CA and shall have appropriate security audit log function for relevant security events. Security audit log shall be automatically generated by the system as far as possible and if the system cannot automatically generate the security audit log, workbook, paper or other physical mechanism should also be used. All security audit logs, electronic or non-electronic, should be properly stored and immediately correctly obtained at execution of auditing. Maintenance of security audit logs shall be handled in accordance with the archiving storage period stipulated in section 4.6.2.

4.5.1 Type of Recorded Event

The CA security audit function shall comprise of the certificate management system and the security audit of the certificate management system depending on the computer operating system. Each audit log shall comprise at least of following items (regardless of whether they are

automatic or manually recorded audit event):

(1) Event type.

(2) Identity of entity or operator that caused the event.

(3) Place and location of event.

(4) Time and date of event.

(5) Results record of CA in execution of certificate issuance and revocation procedures (regardless of success or failure.)

When event happens CA can decide whether to record the audit log electronically or by physical means. The table below shows how the CA shall record the audit events in accordance with the various assurance levels and since these audit events require the CA to record or response for handling, therefore, they are often referred to as the Auditable Event:

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.1 Security audit				
A.1.1 Change of any important audit parameters such as audit frequency, audit event type and new and old parameters, etc.		✓	✓	✓
A.1.2 Any attempt to delete or revise the audit log file		✓	✓	✓

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.2 Identification and Authentication				
A.2.1 Try new role setting regardless of success or failure		✓	✓	✓
A.2.2 Change of maximum tolerance of identity authentication attempt		✓	✓	✓
A.2.3 Maximum failure rate of user attempt to login system with identity authentication		✓	✓	✓
A.2.4 If administrator unlocks the locked account and the account is locked because of multiple failed attempts in identity authentication		✓	✓	✓
A.2.5 Administrator changes the system identity authentication mechanism, for instance, change from password to biometric value		✓	✓	✓
A.3 Key generation				

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.3.1 When CA generates key (not restricted to key generation for single attempt or limited to one attempt)	✓	✓	✓	✓
A.4 Private key login or storage				
A.4.1 Login the private key into the system component	✓	✓	✓	✓
A.4.2 Private key access to the stored CA certificate subject in all key restoration work	✓	✓	✓	✓
A.5. Relying public key additions, deletions and storage				
A.5.1 All relying public key changes including additions and deletions	✓	✓	✓	✓
A.6. Private key export				
A.6.1 Private key export (not including single attempt or limited to one attempt key)	✓	✓	✓	✓
A.7. Certificate registration				

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.7.1 All certificate registration application process	✓	✓	✓	✓
A.8. Revoked certificate				
A.8.1 All certificate revocation application process		✓	✓	✓
A.9. Approval of certificate status change				
A.9.1 Approve or reject certificate status change application		✓	✓	✓
A.10. CA configuration setting				
A.10.1 Any CA security related configuration setting change		✓	✓	✓
A.11. Account management				
A.11.1 Add or delete role and user	✓	✓	✓	✓
A.11.2 User account or role access right revision	✓	✓	✓	✓
A.12. Certificate format dissection management				
A.12.1 All certificate format dissection changes	✓	✓	✓	✓

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.13. CARL and CRL format dissection management				
A.13.1 All CARL AND CRL FORMAT DISSECTION CHANGES		✓	✓	✓
A.14. Others				
A.14.1 Install operating system		✓	✓	✓
A.14.2 Install CA system		✓	✓	✓
A.14.3 Install hardware cryptographic module			✓	✓
A.14.4 Remove hardware cryptographic module			✓	✓
A.14.5 Destroy hardware cryptographic module		✓	✓	✓
A.14.6 Activate system		✓	✓	✓
A.14.7 Attempt login CA application operation		✓	✓	✓
A.14.8 Hardware and software reception			✓	✓
A.14.9 Attempt setting password		✓	✓	✓

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.14.10 Attempt revision password		✓	✓	✓
A.14.11 CA internal data backup		✓	✓	✓
A.14.12 CA internal data restoration		✓	✓	✓
A.14.13 Archival operation (such as generation, rename and relocation, etc.)			✓	✓
A.14.14 Deliver any information to repository for publication			✓	✓
A.14.15 Access CA internal database			✓	✓
A.14.16 Any certificate decryption report		✓	✓	✓
A.14.17 Certificate login token			✓	✓
A.14.18 Token delivery process			✓	✓
A.14.19 Token zeroization		✓	✓	✓
A.14.20 CA key replacement	✓	✓	✓	✓
A.15. CA server setting changes				

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.15.1 Hardware		✓	✓	✓
A.15.2 Software		✓	✓	✓
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓
A.15.5 Security format dissection			✓	✓
A.16. Physical access and site security				
A.16.1 CA computer room for personnel entry/exit			✓	✓
A.16.2 Access CA server			✓	✓
A.16.3 Know or suspect violation of physical security rule		✓	✓	✓
A.17. Abnormalities				
A.17.1 Software error		✓	✓	✓
A.17.2 Software inspection complete failure		✓	✓	✓
A.17.3 Receive inappropriate message			✓	✓
A.17.4 Abnormal route message			✓	✓

Auditable event／assurance level	Level 1	Level 2	Level 3	Level 4
A.17.5 Internet attack (suspect or certain)		✓	✓	✓
A.17.6 Equipment failure	✓	✓	✓	✓
A.17.7 Improper power			✓	✓
A.17.8 UPS failure			✓	✓
A.17.9 Significant and major internet service or access failure			✓	✓
A.17.10 CP violation	✓	✓	✓	✓
A.17.11 CPS violation	✓	✓	✓	✓
A.17.12 System reset clock		✓	✓	✓

4.5.2 Log File Handling Frequency

Audit log should carry out inspection in accordance with following table and interpret major events in the audit report. Inspection work includes verifying whether the audit log has been tempered, and inspect all record items and inspect any alert or abnormalities. All actions taken in line with the inspection audit results shall be documented.

Assurance level	Log file handling frequency
Test level	No stipulations.

Assurance level	Log file handling frequency
Level 1	No stipulations.
Level 2	No stipulations.
Level 3	At least once every other month. Inspect the major security audit logs since last CA audit inspection and conduct further investigation of any possible vicious activities.
Level 4	At least once a month. Inspect the major security audit logs since last CA audit inspection and conduct further investigation of any possible vicious activities.

4.5.3 Audit Log File Storage Period

CA that operates under test assurance level and level 1 the audit log file storage period has no stipulations.

CA that operates under assurance levels 2, 3 and 4 the audit log file should be retained on-site for at least 2 months and handled in accordance with relevant stipulations on record storage and management mechanism in sections 4.5.4, 4.5.5, 4.5.6 and 4.6.

At expiration of storage period of the audit log file only the auditor is authorized to remove the information and no other persons are permitted to do the job for him/her.

4.5.4 Audit Log File Protection

CA that operates under the test assurance level and level 1 is not stipulated for protection of the audit log file.

CA that operates under assurance levels 2, 3 and 4 the electronic audit log system shall comprise of protection mechanism and the manually audited information shall also be protected to ensure no unauthorized reading, revision and deletion.

4.5.5 Audit Log File Backup Procedures

Assurance level	Audit log file backup procedures
Test level	No stipulations.
Level 1	
Level 2	Audit log file shall be backup at least once every month.
Level 3	
Level 4	Audit log file shall be backup at least once every month and backup off-site at least once every month and the relevant off-site backup procedures shall be stated in the CPS.

4.5.6 Security Audit System

The audit system can be in the internal or external CA management system. The audit procedure shall be used at activation of the CA management system and stops only when the CA management system

closes.

4.5.7 Notification of Event Entity

When event happens and recorded by the audit system, latter is not required to notify the event entity that the event has been recorded by the system.

4.5.8 Vulnerability Assessments

CA that operates under assurance levels 3 and 4 shall carry out routine security control vulnerability assessments to ensure the test assurance level, but CA that operates under level 1 and 2 has no stipulations.

4.6 Log Archival Method

4.6.1 Type of Log Event

Record the following information in archival in line with the security requirements of the various assurance levels (CA that operates under the test assurance level has no stipulations.)

Archival data／assurance level	Level 1	Level 2	Level 3	Level 4
CA audit Accreditation data(assumed appropriate)	✓	✓	✓	✓
CPS	✓	✓	✓	✓
Important contracts	✓	✓	✓	✓
System and equipment	✓	✓	✓	✓

configuration setting				
System or configuration setting revision and update content	✓	✓	✓	✓
Certificate application data	✓	✓	✓	✓
Revocation application data		✓	✓	✓
Subscriber identity identification information formulated in section 3.1.9		✓	✓	✓
Document receipt and certificate acceptance		✓	✓	✓
Token activation record		✓	✓	✓
All issued or published certificate	✓	✓	✓	✓
CA key replacement record	✓	✓	✓	✓
All issued or published CARL and CRL		✓	✓	✓
All audit logs	✓	✓	✓	✓
Other explanatory information or application programs used for verifying and used as evidence for the archival content		✓	✓	✓

Document required by auditor		✓	✓	✓

4.6.2 Archival Retention Period

The minimum archival information retention period is as follows:

Assurance level	Minimum retention period
Test level	No stipulations.
Level 1	No stipulations.
Level 2	5 years
Level 3	10 years
Level 4	20 years

If the used storage media cannot attain the above-mentioned retention period, it is required to build up a mechanism for regular archival data conversion to a new storage media. At the same time the application programs for handling archival data shall also maintain a certain period (the length of time should be decided by the competent authority of the CA.)

4.6.3 Archival Protection

Archival data protection is not stipulated for CA that operates under test assurance level and level 1.

For CA that operates under assurance levels 2, 3 and 4 the archival data shall be stored outside the CA and provide appropriate protection and the protection level shall not be lower than the CA site protection level.

4.6.4 Archival Backup Procedures

No stipulations.

4.6.5 Time Stamp Requirements

No stipulations.

4.6.6 Archival Data Sorting System

No stipulations.

4.6.7 Procedures for obtaining and verifying archival data

CA shall state in the CPS the procedures for setting, verifying, formatting and packaging, transferring and storing the archival data.

4.7 Key Changeover

4.7.1 CA Key Changeover

CA private key shall be regularly replaced in accordance with stipulations in section 6.3.2.

If CA itself be revoked certificate it should stop using the private key and is required to replace the key pair.

eCA shall replace the key pair for issuing certificate at least 3 months before expiration of its self-signed certificate and issue a new self-signed certificate before expiration. The Policy Management Committee shall verify the content of the new self-signed certificate and publish before expiration of the old self-signed certificate, and deliver it to the relying

party in accordance with stipulations in section 6.1.4.

The lower CA shall replace the key pair for issuing certificate 2 months before expiration of the certificate. After replacing the key pair the lower CA shall apply for a new certificate with the upper CA before expiration of the lower CA certificate in accordance with stipulations in section 4.1 and issue and publish the lower CA new certificate.

The key replacement time should be decided by the CA in compliance with its CP and whether the CA should continue to apply for cross-certificate with eCA after key replacement depends on the agreement or contract of the CA with Chunghwa Telecom. If the CA requires to continue to apply for cross-certificate with eCA after key replacement, then it is required to follow stipulations in section 4.1 and reserve adequate time for the Policy Management Committee and eCA to process cross-certificate application to ensure that eCA can issue and publish the new cross-certificate of the CA before expiration of the cross-certificate of the CA.

4.7.2 Subscriber Key Changeover

Subscriber private key shall be regularly replaced in accordance with stipulations in section 6.3.2.

If subscriber certificate is being revoked its private key shall stop using and after replacing the key pair it is required to apply for a new certificate with the CA or RA in accordance with stipulations in section 4.1.

Subscriber with assurance levels 2, 3 and 4 and if its certificate is not revoked, the CA or RA can begin to process its application to replace the

key for a new certificate one month before expiration of the subscriber private key and the new certificate application procedures shall follow stipulations in section 4.1.

4.8 Compromise and Disaster Recovery

CA disaster restoration work should place priority to restoring the repository and resume normal provision of certificate status information.

4.8.1 Computing resources, software, and/or data are corrupted

CA shall have the goal of continuous operation and do well all the backup measures in accordance with CP and CPS and reduce losses from disasters to the minimum regarding computer resources, software and data damage and swiftly restore certificate issuance and management operation.

4.8.2 CA Signature Keys signature keys are revoked

CA that operates under assurance levels 2, 3 and 4 shall state in the CPS or relevant documents the restoration procedures for CA signature key certificate revocation and swiftly restore certificate issuance and management operation.

4.8.3 CA Signature Keys are compromised

CA that operates under assurance levels 2, 3 and 4 shall state the restoration procedures in CPS or relevant documents for CA signature key decryption and swiftly restore certificate issuance and management operation.

4.8.4 Secure Facility impaired after a Natural or Other type of Disaster

CA that operates under assurance levels 2, 3 and 4 shall state in CPS or relevant documents the steps for rebuilding the CA security installations after natural or other disasters.

4.9 CA Termination

CA should terminate its service in accordance with the relevant regulations of the Electronic Signature Law.

5 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Control

5.1.1 Physical Locations and Structure

Except for CA that operates under test assurance level and level 1 where stipulations are not required, the physical location and structure of the computer room for CA that operates under assurance level at or above level 2 shall conform to the computer room installation standard for storage of highly important and sensitive information in conjunction with door security, security, intrusion detection and video monitoring and other physical security mechanisms to prevent unauthorized access to the relevant equipment of the CA.

5.1.2 Physical Access

Except for CA that operates under test assurance level and level 1 where stipulations are not required, CA that operates under assurance level at or above level 2 shall exercise physical control of CA equipment after installation and activation of the cryptographic module to prevent unauthorized access. Relevant equipment of CA shall be put under physical control even if the cryptographic module is not installed or activated to minimize the risk of equipment being illegally opened or damaged.

Stipulations of physical control at various assurance levels are explained below:

Physical control stipulations of CA that operates under assurance levels 1 and 2:

(1) Make sure to prevent unauthorized intrusion.

(2) Make sure the portable storage media with sensitive documentary information and documentation are stored in a secure place.

Physical control stipulations of CA that operates under assurance levels 3 and 4:

(1) Build an all-weather manual or electronic monitoring equipment to prevent unauthorized intrusion.

(2) Regularly maintain and inspect the accessed log files.

(3) Have at least two persons for joint execution of physical control of the computer system and cryptographic module.

Since eCA shall issue certificate of all assurance levels therefore its security mechanism of equipment environment shall follow physical control stipulations of assurance level 4. There are no stipulations on physical control of CA that operates under test assurance level but it shall be explained in the CPS.

Before leaving the CA computer room it is necessary to inspect the following items to prevent access by unauthorized personnel to the CA computer room:

(1) Have appropriate security cabinet box.

(2) Normal operation the physical security system (such as door locks

and other door security.)

5.1.3 Power and Air-conditioning

Except for CA that operates under test assurance level and level 1 where stipulations are not required, CA that operates under assurance level at or above level 2 shall have sufficient power and air-conditioning for adequate backup installations to support the relevant systems of CA to ensure normal operation or power off under influence of external factors. At the same time, it shall provide UPS with at least 6 hours of backup power to provide backup information of the repository (including issued certificate and CRL.)

5.1.4 Flood Prevention and Protection

CA location must be away from flood damage.

5.1.5 Fire Prevention and Protection

Except for CA that operates under test assurance level and level 1 where stipulations are not required, CA that operates under assurance level at or above level 2 shall have automatic fire alarm detection function for its computer room and the system can automatically activate the fire extinguishing equipment and install manual switches at entrances and exits to permit manual operation by personnel at site in emergencies.

5.1.6 Media Storage

Except for CA that operates under test assurance level and level 1 where stipulations are not required, CA that operates under assurance level at or above level 2 shall protect the relevant storage media of the system from

accidental damage (such as flood, fire and magnetic field, etc.)

5.1.7 Waste Handling

No stipulations.

5.1.8 Off-site Backup

No stipulations.

5.2 Procedure Control

5.2.1 Relying Role

CA shall arrange relying role to be responsible for execution of relevant tasks and use it as the CA relying foundation and the fairness of CA could be lowered if the security goal failed to be achieved because of accidents or human errors. CA should take following two methods to enhance security:

(1) Guarantee personnel of each role has received appropriate training and is fully reliable.

(2) Appropriately separate each task and each task should be assigned to more than one person in order to prevent one person to carry out vicious activities.

The stipulated relying roles are as follows:

(1)Administrator: Responsible for installation, setting and maintenance of CA relevant systems and establishment and maintenance of the system subscriber accounts and setting audit parameters and generation of component key.

(2)Officer: Issues and revokes certificate.

(3)Auditor: Inspects and maintains audit log.

(4)Operator: Executes system backup and failure troubleshooting.

5.2.1.1 Administrator

The administrator is principally responsible for:

(1) Installation, setting and maintenance of CA relevant systems.

(2) Establish and maintain system user accounts.

(3) Setting audit parameters.

(4) Generate and backup CA key.

5.2.1.2 Officer

The officer is principally responsible for:

(1) Registering new certificate subscriber and processing applications for certificate issuance.

(2) Verifying certificate subscriber identity and certificate information is correct.

(3) Reviewing and executing certificate issuance.

(4) Processing application, reviewing and executing certificate revocation.

5.2.1.3 Auditor

The auditor is principally responsible for:

(1) Inspection, maintenance and archival of audit log.

(2) Execute or monitor internal audit to ensure CA abides with CPS stipulations.

5.2.1.4 Operator

The operator is principally responsible for:

(1) Physical security control of the system (such as computer room door security management, fire and flood prevention, air-conditioning system, etc.)

(2) Daily operation and maintenance of the system equipment.

(3) System backup and restoration operation.

(4) Storage media update.

(5) System software and hardware update.

(6) Internet and website maintenance: Establish system security and anti-virus protection mechanism and detection and circulation of internet security event.

5.2.2 Role Assignment

Certification Authority (CA) role assignment principle is as follows:

Assurance level	Role assignment principle
Test level	No stipulations.
Level 1	No stipulations.

Assurance level	Role assignment principle
Level 2	Four relying roles as stipulated in section 5.2.1 and permits one person to have more than one role but issuer and administrator shall not be concurrently held.
Level 3	Four relying roles as stipulated in section 5.2.1 and permits one person to have more than one role but issuer shall not concurrently be administrator or auditor.
Level 4	Four relying roles as stipulated in section 5.2.1 and permits one person to have more than one role but personnel and role assignment shall conform to following stipulations: (1)Administrator, issuer and auditor shall not concurrently hold overlapping roles but can play the role of operator. (2)Any one role shall not permit execution of self-audit function.

5.2.3 Number of persons required per task

To ensure optimum security of CA equipment and maintenance personnel role assignment shall follow stipulations in section 5.2.2 and the required number of person per task shall be stated in the CPS.

5.2.4 Identification and Authentication of Each Role

Except for CA that operates under test assurance level and level 1 where stipulations are not required, CA that operates under assurance level at or above level 2 relevant CA personnel shall be identified and verified his/her identity before executing role assignment task.

5.3 Personnel Control

CA shall be genuinely in control of relevant personnel of CA or RA operation and personnel task assignment shall conform to following security control requirements:

(1) Assign work in written form.

(2) Stipulate conditions for task execution by laws and regulations or contract.

(3) Accept relevant training for task.

(4) Stipulate non-disclosure of sensitive CA relevant security information and certificate subscriber data by laws and regulations or contract.

(5) Task assignment shall conform to the principle of conflict of interests.

5.3.1 Background, qualifications, experience, and security clearance requirements

CA shall carry out personnel identification operation and select loyal, reliable, righteous and R.O.C. citizens as personnel of relying roles and state the relevant rules for personnel qualifications, selection, supervision and auditing in the CPS.

5.3.2 Background Inspection Procedures

Background inspection procedures shall be stated in the CPS.

5.3.3 Educational Training Requirements

Relevant CA personnel shall receive following educational training:

(1) CA and RA security authentication mechanism.

(2) CA system uses PKI software.

(3) Responsible for execution of PKI tasks.

(4) Procedures for disaster restoration and continuous business operation.

5.3.4 Personnel Educational Training Requirements and Frequency

Relevant CA personnel shall be familiar with CA relevant work procedures and changes in laws and regulations. In the event of any major changes such as upgrade of CA software and hardware, change of work procedures and equipment replacement CA personnel shall receive educational training and record the training details.

New employees shall also receive educational training accordingly and CA shall annually carry out inspection of training of relevant personnel.

5.3.5 Job Rotation Frequency and Sequence

No stipulations.

5.3.6 Sanction of Unauthorized Actions

CA shall formulate appropriate management methods to prevent unauthorized access to information by personnel and publish the relevant

rules in the CPS. CA shall appropriately manage and punish personnel who have violated the CP or CPS.

Relevant personnel in execution of eCA and the repository host shall be appropriately managed and punished for violation of CP or CPS or other eCA published procedures.

5.3.7 Contracting personnel requirements

Contractor personnel employed to perform relevant CA tasks shall conform to CA CPS stipulations.

5.3.8 Documentation supplied to personnel

CA shall provide CP, CPS and other rules, policies, contracts and relevant documents to personnel of the CA and RA.

6 Technical Security Control

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic module used for CA certificate shall be approved by Chunghwa Telecom with cryptographic module of equivalent security level for key generation.

Random number used in the process of key generation shall have a length and randomness that made it computationally infeasible for calculating out the same random series even if adequate information and equipment are provided.

The private key stored in the cryptographic module shall be prevented from leaking outside. If the private key is generated in the cryptographic module the key should be stored in the cryptographic module or encrypted and stored in the host. If the private key is generated outside the cryptographic module the key should be imported into the cryptographic module without leaving the environment for key generation and the environment assures that no one can use any method to get the generated private key without being detected, and after the private key is being stored in the cryptographic module the key should immediately be deleted from the key-generation environment.

CA shall take appropriate measures to ensure the subscriber public key administered by the CA is the only one key in ePKI.

6.1.2 Private Key Secure Delivery to Subscriber

It is not required to deliver the private key if it is generated and stored in the subscriber cryptographic module.

If the entity (such as certificate subscriber or IC Card Issuance Center) directly generates key from its owned Token or generates key from another key generator and deliver the key to the entity token, then the entity is considered to have owned the private key when the key is generated and accepted by the entity. If the foregoing entity is not the certificate subject for certificate application, then it should securely deliver the private key to the certificate subject with auditable methods to complete transfer of the private key.

For all assurance levels, if the hardware for storing the key is delivered to subscriber it is required to make sure the correct token and its Activation Data is delivered to subscriber. CA shall keep a record to verify that subscriber has received the said token. In using any secret sharing (such as password or PIN code) mechanism, the mechanism shall ensure only the applicant and eCA or its subordinate CA is the only entity that owns the secret.

If the private key is generated by the CA or RA or a relying third party, then the cryptographic module shall be securely delivered to the subscriber and latter shall confirm receipt of the private key. The storing location of the cryptographic module and the status tracking record shall be properly stored until at least subscriber has confirmed receipt of the cryptographic module.

Under any circumstances, except the subscriber, other persons shall not obtain or in control of the signature private key. Any entity that generates signature private key for subscriber shall also not retain any backup copy of the key.

6.1.3 Public Key Securely Delivered to CA

At verifying the identity of subscriber by CA, the subscriber shall deliver the public key to the CA and the ways of delivery include:

(1) RA sends out electronic message for certificate application.

(2) In generating key by a third party the CA or RA shall obtain the subscriber public key through an auditable secure channel.

(3) Can also be accomplished by other secure electronic mechanism.

(4) Can also be accomplished by secure non-electronic methods including (but not limited to) via registered mail or express courier of floppy disk (or other storage media.)

6.1.4 CA Public Key Securely Delivered to the Relying Party

The eCA public key shall be available at all time. The subordinate CA shall use a relying method to deliver the eCA self-signed certificate or public key to the user. The relying certificate delivery method comprises of following:

(1) CA uses a token to store the eCA self-signed certificate or public key and securely deliver to the relying party.

(2) Using special out-of-band delivery of eCA self-signed certificate or

public key.

(3) Using special out-of-band delivery of eCA self-signed certificate or public key hash value or fingerprint for the user to compare (to publish online in-band with the certificate hash value or fingerprint is not considered a viable secure channel.)

(4) Download from website the eCA SELF-SIGNED CERTIFICATE OR PUBLIC KEY WITH SAME ASSURANCE LEVEL OR HIGHER ASSURANCE LEVEL.

(5) Other methods approved by the Policy Management Committee.

Aforementioned special out-of-band shall be stated in the eCA CPS.

eCA issued subordinate CA certificate shall be published in the CA repository.

6.1.5 Key Length

Assurance level	Symmetric key	Public key
Test level	Shall at least possess or other type of key with equivalent security strength such as bit.	Shall at least use bit key or other type of key with equivalent security strength such as bit.
Level 1		
Level 2		
Level 3		

Level 4		Shall use at least 2048 bit RSA key or other type of key with equivalent security strength (such as ECC 224 bit.)

6.1.6 Public Key Parameter Generation

As regards RSA algorithm the public key parameter shall be Null; as for other algorithms the public key parameter shall follow relevant international standard.

6.1.7 Key Parameter Quality Inspection

As regards RSA algorithm, it is not required to do parameter quality inspection but must do prime number testing and the CA shall state in the CPS how to carry out the relevant testing.

As regards other algorithms follow the international standard including prime number testing.

6.1.8 Key Generated by Software or Hardware

Any random number used for key generation shall be approved by Chunghwa Telecom. Subscriber random number, key pair and symmetric key generation using software or hardware stipulations are listed in the table below:

Assurance level	Key generation mechanism
Test level	Software or hardware

Level 1	Software or hardware
Level 2	Software or hardware
Level 3	Software or hardware
Level 4	Only limited to hardware

6.1.9 Key Usage Purposes

The certified public key in certificate shall state its key usage in X.509 certificate keyUsage extension (signature or encryption). A digital signature (including authentication) certificate shall set digitalSignature bit; certificate for encryption use shall set keyEncipherment or dataEncipherment bit. Certificate of CA itself shall set two key usage bit: cRLSign and keyCertSign.

Certificate with assurance levels of test level, level 1,2 and 3 can use a single key simultaneously for encryption and signature to support certain old version Secure Multipurpose Internet Mail Extensions (S/MIME) application software. Except stated otherwise by CP such Dual-Use certificate shall be generated and managed in accordance with signature usage certificate stipulations and shall not set Non-Repudiation Key Usage bit, particularly not being used in signature certified important information. As for subordinate CA, regardless of the assurance level, two types of key shall be issued for certificate to subscriber, one for data encryption use, and the other for digital signature and identity authentication use.

6.2 Private Key Protection

6.2.1 Cryptographic Module Standard

The Policy Management Committee shall decide the cryptographic module authentication standard used by ePKI wherein the security requirement of the cryptographic module should comply with U.S. FIPS 140-2 series or the standard of equivalent security strength and the cryptographic module used by CA for issuing certificate shall pass the foregoing security certificate standard.

Regarding the various PKI entities, except that the subscriber shall comply as far as possible, the remaining entities should follow the minimum security requirements as listed in the table below for cryptographic module but can use higher assurance levels and the level used in the table follows the U.S. FIPS 140-2 series definitions.

Entity/assurance level	eCA	Subordinate CA	RA	Subscriber
Test level	N/A	No stipulations	No stipulations	No stipulations
Level 1	N/A	Level 1 (hardware or software)	Level 1 (hardware or software)	No stipulations
Level 2	N/A	Level 2 (hardware or	Level 1 (hardware or	Level 1 (hardware or

		software)	software)	software)
Level 3	N/A	Level 2 (hardware)	Level 2 (hardware)	Level 1 (hardware or software)
Level 4	Level 3 (hardware)	Level 3 (hardware)	Level 2 (hardware)	Level 2 (hardware)

6.2.2 Multi-Person Control of Key

CA signature private key for issuing certificate of assurance levels 3 and 4 shall conform to the multi-person control procedure as stipulated in Chapter 5.

6.2.3 Private Key Escrow

Private key for signature shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 CA Signature Private Key Backup

CA that operates under assurance levels 3 and 4, its signature private key shall be backup under multiple control procedures and store in the backup site; the key backup procedures shall be stated in the CPS.

6.2.4.2 Subscriber Signature Private Key Backup

For certificate with assurance levels 1, 2 and 3, subscriber signature private key can be backup or duplicated but shall be controlled by the subscriber.

For certificate with assurance level 4, subscriber signature private key shall not be backup or duplicated.

6.2.5 Private Key Archival

Signature private key shall not be archived.

6.2.6 Private Key Imported to Cryptographic Module

In accordance with stipulations in section 6.1.1.

6.2.7 Private Key Activation Method

Private key stored in the cryptographic module shall verify identity of the activator at activation. The acceptable authentication methods include (but not limited to) passphrase, personal token, PIN code or biometric identification, but the imported activation data shall not be disclosed (should not be displayed.)

The activated private key shall not be left unattended or allow unauthorized access.

6.2.8 Private Key deactivating Method

Cryptographic module not in use shall stop operation; through manual logout procedure or after certain period of time without operation (length of time is stipulated in the CPS) will automatically stop operation. If the hardware cryptographic module is no longer in use it shall be separated from the host and stored in a secure place.

6.2.9 Private signature Key Destruction Method

If the signature private key and its backup are no longer needed or certificate expires or revoked, the signature private key shall be destroyed. As for the software cryptographic module, it is required to duplicate the data onto the memory or storage media originally occupied by the signature private key. As for the hardware cryptographic module, it must be "Zeroized" but it is not required to physically destroy the module.

6.3 Other Rules for Subscriber Key Pair Management

Though it is technically feasible to use a single key simultaneously for signature and encryption, it is recommended to issue two key pairs certificate to subscriber, except for conformance to old version application system as stipulated in section 6.1.9, one key pair for data encryption and the other key pair for digital signature and identity authentication, regardless of what assurance level.

Private key used by subscriber for signature and identity authentication shall not be escrowed, archived or backup; Subscriber backed CA shall request for escrow, archival or backup for encryption of private key to facilitate duties.

6.3.1 Public Key Archival

After certificate being archived it is not required for public key archival.

6.3.2 Public Key and Private Key Usage Period

6.3.2.1 CA Public Key and Private Key Usage Period

CA public key and private key have different key strength and

assurance levels and their usage periods are explained below:

(1) RSA 4096 bit or other type of public key pair with equivalent security strength (such as ECC 300 bit): the maximum private key usage period is 15 years; and the maximum public key certificate valid period is 30 years.

(2) RSA 2048 bit or other type of public key pair with equivalent security strength (such as ECC 224 bit): the maximum private key usage period is 10 years; and the maximum public key valid period is 20 years.

(3) RSA 1024 bit or other type of public key pair with equivalent security strength (such as ECC 161 bit): the maximum private key usage period is 5 years; and the maximum public key valid period is 10 years.

Signature private key for eCA to sign certificate the key life cycle shall not exceed half of its self-signed certificate and its self-signed certificate life cycle shall not exceed 30 years.

Certificate signed by eCA to its subordinate CA its life cycle plus the life cycle of the signature private key for eCA to sign certificate shall not exceed the eCA self-signed certificate life cycle.

6.3.2.2 Subscriber Public Key and Private Key Usage Period

Subscriber key usage period is based on its key length, if the key has equivalent security strength as RSA 1024 bit, then the private key maximum usage period is 5 years; if the key has equivalent security

strength as RSA 2048 bit, then the private key maximum usage period is 10 years. The total valid period of certificate (including extension) is at most same as the key usage period.

6.4 Activation Data Protection

6.4.1 Activation Data Generation

Activation data for decryption of CA or certificate subscriber private key and other relevant access control mechanism shall be appropriately protected. CA that operates under assurance levels 1, 2 and 3 its activation data should be self-selected by the user. CA that operates under assurance level 4 shall accept user's biometric data or use the intensified security mechanism of cryptographic module. If Password is used to activate data, generation of the password shall conform to the main points of data security management regulations. And if the activated data shall be delivered it shall be through an appropriate secure channel.

6.4.2 Activation Data Protection

Activation data for decryption of the private key shall use a combination of password and access control security mechanism for protection and prevent disclosure. The activation data can be stored with biometric features or memory. If required to leave record, it shall use a cryptographic module with equivalent data security assurance level for protection to ensure its security. If the number of login failure exceeds the maximum preset value stipulated in the CPS, the protective mechanism shall be able to immediately lock the account or terminate the application program.

6.4.3 Other Activation Data Rules

No stipulations.

6.5 Computer Software and Hardware Security Control Measures

6.5.1 Specific Computer Security Technical Requirements

CA that operates under assurance levels 3 and 4 and its relevant supportive systems shall comprise of following functions and such computer security functions can be provided by the protective measures of the operating system or a combination of the operating system, software and hardware.

(1) Login with identity authentication.

(2) Provide discretionary access control.

(3) Provide security audit capability.

(4) Access control restrictions for the various certificate services and PKI relying roles.

(5) Possess PKI relying role and relevant identity identification and authentication.

(6) Use cryptographic technology to ensure each telecommunication and database security.

(7) Possess PKI relying role and relevant secure and relying channel for identity identification.

(8) Possess complete procedures and security control protection.

(9) CA equipment shall be built on the operation platform that has passed security appraisal and the relevant CA systems (hardware, software and operating system) shall operate under a configuration that has passed security appraisal.

6.5.2 Computer Security Appraisal

No stipulations.

6.6 Life Cycle Technical Control Measures

6.6.1 System development controls

CA system development control measures are explained below:

Assurance level	System R&D Control Measures
Test level	No stipulations.
Level 1	No stipulations.
Level 2 Level 3 Level 4	(1) CA used software must use fair software engineering development method for development such as using Capability Maturity Model(CMM). (2) CA hardware and software must be for dedicated use and must not install other application system not related to operation (including hardware device, internet linking or

Assurance level	System R&D Control Measures
	component software.) (3) Must prevent installation of vicious software in the CA equipment. CA operation can only use CP licensed components. (4) Hardware and software used in the RA must be inspected for vicious programs before using it the first time and regularly scan the program.

6.6.2 Security management controls

Assurance level	Security Control Measures
Test level	Must record and control CA relevant system configuration and any revision and function upgrade and possess detection of unauthorized revision of CA software or mechanism of configuration. At first installation of CA software it is required to make sure the supplier has provided unrevised and correct version.
Level 1	
Level 2	
Level 3	

Assurance level	Security Control Measures
Level 4	Must record or control CA relevant system configuration and any revision and function upgrade and possess detection of unauthorized revision of CA software or configuration mechanism. At first installation of CA software, it is required to make sure the supplier has provided unrevised and correct version. CA shall verify the completeness of CA software at least once a month.

6.6.3 Life Cycle Security Ratings

No stipulations.

6.7 Network Security Controls

eCA host and the internal repository shall not be linked with any external internet. But the eCA external repository is linked to the internet to provide uninterrupted service (except for necessary maintenance or backup). Manually deliver the internal repository information to the external repository and all information (certificate and CARL) shall be protected with digital signature. The external repository shall be protected with update of the system repairing program, weakness scan, intrusion detection system, firewall, filtering router, etc. to prevent attack to stop service and intrusion.

6.8 Cryptographic Module Engineering Controls

In accordance with stipulations in sections 6.1 and 6.2.

7 CERTIFICATE AND CARL/CRL PROFILES

7.1 Certificate Profile

7.1.1 Version numbers

CA shall issue X.509 v3 version certificate and its version number is 2.

7.1.2 Certificate Extensions

Formulate rules for the use, processing and field value setting of the Certificate Extensions in the certificate format dissection. Exercise appropriate control of the CPS framework through certificate format dissection to provide adequate flexibility to conform to the requirements of different CA and social groups.

eCA issued certificate shall comply with the rules of the certificate and CRL format dissection of Chunghwa Telecom ecommerce Public Key Infrastructure Certification Technical Standard and if its subordinate CA issued certificate belongs to the third assurance level shall also comply with the rules of the certificate and CRL format dissection; and if the assurance levels belong to levels 1 and 2 then it shall conform to the RFC 2459 rule. And if self extensions are used it is required to state in the CPS and at the same time ensure that Critical self extensions shall be interoperable with its social groups in application service.

7.1.3 Algorithm Object Identifiers

The issued certificate shall use the following algorithm OID in issuing certificate:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

The issued certificate shall use the following OID to identify generation of the subject key algorithm:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name forms

The two field values of the certificate subject and the issuer shall use the X.500 only Distinguished Name and the name attributes shall comply with the RFC 2459 regulations.

7.1.5 Name constraints

No stipulations.

7.1.6 Certificate policy object identifier

The issued certificate shall use the CP object identifier and at the same time the CP object identifier shall have the same certificate assurance level.

7.1.7 Usage of Policy Constraints extension

No stipulations.

7.1.8 Policy Qualifiers Syntax and Semantics

The issued certificate shall not comprise of Policy Qualifiers.

7.1.9 Processing semantics for the critical certificate

policy extension

The semantic processing of critical CP extensions used for issuing certificate shall comply with the certificate and CRL dissection rules.

7.2 CARL/CRL Profile

7.2.1 Version Numbers

The issued CARL and CRL shall conform to the X.509 v2 regulations.

7.2.2 CARL and CRL entry extensions

The CARL/CRL format dissections stipulate that each extension shall comply with the certificate and CRL format dissection regulations.

8 CP and CPS Maintenance

8.1 Change Procedures

The Policy Management Committee shall inspect the CP at least once a year and the CA shall inspect the CPS at least once a year to ensure its assurance level. If CP revision does not affect the CP declared certificate usage purpose and assurance level the CP OID does not require revision but if the CP OID has changed the CPS shall make corresponding revision.

8.1.1 Change Items Not for Notification at Change

Re-layout of CP and CPS will not be notified.

8.1.2 Notified Change Items

Notified change items shall be stated in the CP and CPS.

8.1.2.1 Change Items

Extent of effect to subscriber or relying party because of CP item changes evaluated by the Policy Management Committee:

(1)Must be published 15 calendar days in advance before revision for major effect.

(2)Must be published 7 calendar days in advance before revision for minor effect.

8.1.2.2 Notification Mechanism

The Policy Management Committee and CA shall publish in the

eCA and CA repositories for change items that could produce major effect to subscriber and CA shall state in its CPS the notification mechanism of the change items.

8.1.2.3 Opinion Response Deadline

The opinion response deadline to change items is stipulated in section 8.1.2.1.

(1)In accordance with section 8.1.2.1 the response deadline is 7 calendar days for major effect.

(2)In accordance with section 8.1.2.1 the response deadline is 3 calendar days for minor effect.

CA shall state in the CPS the opinion response deadline.

8.1.2.4 Opinion Handling Mechanism

The Policy Management Committee is responsible for handling relevant opinions to the CP and CA shall state the opinion handling mechanism in the CPS.

8.1.2.5 Final Publication Deadline

Change items published by CP shall be revised in accordance with stipulations in sections 8.1.2.2 and 8.1.2.3 and shall be published for at least 7 calendar days in accordance with stipulations in section 8.1.2.1 until CP revision takes effect and the CA shall state the final publication deadline in the CPS.

8.2 Publication and Notification Rules

CP publication and subsequent revision must be published in the eCA repository 7 calendar days after approval by the Policy Management Committee and the CA shall state the publication and notification rules in the CPS.

8.3 CP and CPS Revision Procedures

The CA CPS shall comply with relevant laws and regulations and conform to CP regulations and approved by Chunghwa Telecom and the Electronic Signature Law Competent Authority the Ministry of Economic Affairs. After publication of CP revision the CA CPS shall make corresponding revisions and submit to the Policy Management Committee and the Electronic Signature Law Competent Authority the Ministry of Economic Affairs for approval.