Public Certification Authority
Certification Practice Statement

Version 1.3

Chunghwa Telecom Co., Ltd.

2008/04/18

Chunghwa Telecom

Table of Contents

ABSTRACT I

1 GENERAL GUIDELINES 1

1.1 CPS APPLICABILITY 1

1.2 VERSION IDENTIFICATION 1

1.3 KEY MEMBERS AND CERTIFICATION APPLICABILITY 2

1.4 CONTACT 7

2 GENERAL PROVISIONS 8

2.1 OBLIGATIONS AND RESPONSIBILITIES 8

2.2 LEGAL RESPONSIBILITY 11

2.3 FINANCIAL RESPONSIBILITY 15

2.4 APPLICABLE LAW AND RESOLUTION OF DISPUTES 16

2.5 FEES 16

2.6 PUBLICATION AND REPOSITORY 17

2.7 AUDITING METHODS 19

2.8 INFORMATION CONFIDENTIALITY SCOPE 21

2.9 INTELLECTUAL PROPERTY RIGHTS 22

3. IDENTIFICATION AND VERIFICATION 24

3.1 PRELIMINARY REGISTRATION 24

3.2 CERTIFICATION KEY REPLACEMENT AND EXTENSION 28

3.3 CERTIFICATION REVOCATION KEY REPLACEMENT 29

3.4 CERTIFICATION REVOCATION 29

3.5 CERTIFICATION TEMPORARY SUSPENSION AND RESUMPTION FOR USE 29

4 OPERATION REQUIREMENTS 30

4.1 CERTIFICATION APPLICATION PROCEDURES 30

4.2 CERTIFICATION ISSUANCE PROCEDURES..... 30

4.3 CERTIFICATION ACCEPTANCE PROCEDURES 31

4.4 CERTIFICATION TEMPORARY SUSPENSION AND REVOCATION..... 32

4.5 SECURITY AUDITING PROCEDURES 37

4.6 RECORD FILING 40

4.7 KEY REPLACEMENT 43

4.8 RESUMPTION PROCEDURES FOR KEY DECRYPTION OR DISASTER .. 44

4.9 THE PUBLICCA OF CHUNGHWA TELECOM TERMINATES SERVICE ... 45

5 CONTROL OF PHYSICAL ENTITY, PROCEDURES AND PERSONNEL SECURITY 47

5.1 PHYSICAL CONTROL 47

5.2 PROCEDURAL CONTROLS 50

5.3 PERSONNEL CONTROL 55

6 TECHNICAL SECURITY CONTROL 59

6.1 KEY PAIR GENERATION AND INSTALLATION 59

6.2 PRIVATE KEY PROTECTION 61

6.3 OTHER KEY POINTS OF KEY PAIR MANAGEMENT 64

6.4 PROTECTION OF ACTIVATED INFORMATION..... 65

6.5 COMPUTER SOFTWARE AND HARDWARE CONTROL MEASURES 66

6.6 LIFE CYCLE TECHNICAL CONTROL 66

6.7 INTERNET SECURITY CONTROL MEASURES 67

6.8 CRYPTOGRAPHIC MODULE SECURITY CONTROL MEASURES 68

7 CERTIFICATION AND CRL FORMAT DISSECTION 69

7.1 CERTIFICATION FORMAT DISSECTION 69

7.2 CRL FORMAT DISSECTION 71

8 CPS MAINTENANCE 72

Abstract

Chunghwa Telecom Co., Ltd. has formulated the Certification Practice Statement (hereinafter referred to as the CPS) of the Public Certification Authority of Chunghwa Telecom（hereinafter referred to as the PublicCA）in accordance with Article 11 of the Digital Signature Law and the Specific Guidelines for the Certification Practice Statement promulgated by the Ministry of Economic Affairs. Formulation and revision of the CPS shall be published in the company website after approval by the competent government department for issuance of certification service.

I. Competent department approved number: Jingshangzi. 09702408330.

II. Types of issued certification:

Certification of the natural person, organization, equipment or application software.

III. Assurance Classes of certification:

The Public Certification Authority of Chunghwa Telecom operates in accordance with relevant regulations of the Certification Policy of the public key infrastructure of the Chunghwa Telecom ecommerce (hereinafter referred to as CP) and issues Class 1, Class 2 and Class 3 certification defined by the issuing CP in accordance with the identity verification procedures of the applicant to different classes of natural person,

organization, equipment or application software (refer to section 1.3.5.1).

IV. Applicable scope:

Certification issued by the PublicCA applies to identity certification and data encryption required by e-commerce and financial network trading.

Subscribers and related relying parties of the PublicCA must exercise prudence in using the certification issued by the PublicCA and must not depart from the CPS, relevant laws and regulations and restrictions and prohibitions of the certification applicable scope stipulated in the contract between the PublicCA and subscribers and the relevant relying parties.

V.Important matters of relevant legal responsibilities:

(1)Damage indemnification responsibility of the PublicCA and the Registration Authority

In the event of damage to subscribers or relying parties in relevant certification operations of the PublicCA and the registration authority due to intentional or errors in noncompliance with the CPS and relevant operation regulations, the PublicCA or the RA shall respectively be responsible for indemnity. The subscriber is entitled to damage indemnity in accordance with relevant provisions of the contract with the PublicCA or the RA; and the relying party is entitled to damage indemnity with the relevant laws

and regulations.

(2) Exemption of responsibility of the PublicCA

For damages caused by noncompliance of the CPS, relevant laws and regulations by the subscriber and the relying party and noncompliance of the contract between the PublicCA and the subscriber and the relevant relying party or any damages that occurred not attributable to the PublicCA shall be accountable by the subscriber or the relying party for damage indemnity.

(3) Exemption of responsibility of the registration authority

For reasons attributable to the subscriber that caused damage to the relying party or occurrence of any damages not attributable to the registration authority shall be accountable to the subscriber or relying party for damage indemnity.

For damages caused by the subscriber or relying party because of noncompliance of the CPS and relevant laws and regulations, and because of noncompliance of the contract between the registration authority and the subscriber and the relying party or any damages not attributable to the registration authority shall be accountable to the subscriber or the relying party for damage indemnity.

(4) Exemption provisions

For damages caused by the PublicCA and the RA for

reasons of force majeure or other reasons not attributable to the PublicCA and the RA, the PublicCA and the RA are not accountable for any legal responsibility. For damages caused because of deviation from the applicable scope with specified restrictions on the use of certification the PublicCA and the RA are not accountable for any legal responsibility.

Requirements of PublicCA system maintenance, conversion and expansion must be published in the repository in advance to temporarily suspend portions of the certification service, the subscriber or the relying party shall not demand for damage indemnity from the PublicCA.

(5) Financial responsibility

The PublicCA has financial guaranty from Chunghwa Telecom Co., Ltd.; the PublicCA shall carry out financial auditing in accordance with relevant laws and regulations.

(6) Subscriber obligations

The subscriber must properly store and use his/her private key. Temporary suspension of use, revocation, extension or re-issuance of subscriber certification must conform to stipulations of chapter four of the CPS and must assume obligations of using the certification before any changes.

VI. Other important matters

(1)The registration work of RA affiliated to the PublicCA is authorized by the PublicCA.

(2)The subscriber must comply with the relevant regulations of the CPS and ensure all provided application information is correct.

(3)In reasonably relying on the PublicCA for issuance of certification the relying party must verify the correctness, effectiveness and usage restrictions of the relying certification.

(4)The company shall assign a fair third party for auditing operation of the Public Certification Authority of Chunghwa Telecom

1 General Guidelines

The title of this document is Public Certification Authority Certification Practice Statement of Chunghwa Telecom; hereinafter referred to as the CPS). The CPS is formulated in accordance with the Certification Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure; hereinafter referred to as the CP).

The PublicCA is the Level 1 Subordinate CA of Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI), and is responsible for issuance and management of the certification of natural person, organization, equipment or application software in the Infrastructure. The Chunghwa Telecom ePKI Root Certification Authority (eCA) is the top certification authority of the Infrastructure and the relying source of the Infrastructure and is responsible for operation and setup by Chunghwa Telecom Co., Ltd. The relying parties can directly rely on certification by the Chunghwa Telecom ePKI Root Certification Authority.

1.1 CPS applicability

The practical operation rules specified in the CPS apply to the PublicCA, Registration Authority, Subscribers, Relying Parties and the Repository.

1.2 Version identification

The CPS version is 1.3 and the version publishing date is April 18, 2008. You can obtain the latest version of the CPS from the website below:

http://publicCA.hinet.net

The corresponding CP object identification codes of the CPS are given in the

table below:

Assurance level	Object identification code	Object identification value
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}

1.3 Key Members and Certification Applicability

The relevant members of the PublicCA comprise of:

(1) The Public Certification Authority of Chunghwa Telecom

(2) Registration Authority

(3) Repository

(4) Subscribers and Relying Parties

1.3.1 The Public Certification Authority of Chunghwa Telecom

The Public Certification Authority of Chunghwa Telecom is being set up and operated by Chunghwa Telecom Co., Ltd. and issues certification for the natural person, organization, equipment and application software in accordance with the stipulated operation of the CP.

1.3.2 Registration Authority

The Registration Authority is responsible for collection and verification of

subscriber identity and registration work of relevant certification related information. The Registration Authority is formed by multiple RA counters authorized by the organization approved by the PublicCA. Each RA counter has an RA Officer (RAO） responsible for certification application and revocation operations.

1.3.3 Repository

The PublicCA Repository is responsible for publication and storage of certification and CRL issued by the PublicCA and provide subscribers and relying parties inquiry service. The Repository provides 24 hours service and the Repository website is: http://publicCA.hinet.net。

1.3.4 Subscribers and Relying Parties

1.3.4.1Subscriber

Refer to the individual who has applied and obtained certification issued by the PublicCA. The subscriber's relation with the certification entity is given in the table below:

Certification entity	Subscriber
Natural person	himself
Organization	Trustee of authorized organization
Equipment	Owner of equipment
Application software	Owner of application software

Generation of the subscriber public key pair must conform to the stipulations of section 6.1.1 of the CPS and the subscriber must possess the power and capability of independently controlling the corresponding private keys.

1.3.4.2 Relying party

Relying party refers to the third party that believes the linking relation between the subject of the certification entity and the public key. The relying party must verify the effectiveness of certification corresponding to certification of CA and certification status information, and proceed to use certification for following operations only after verification of the effectiveness of certification:

(1) Verify the completeness of an electronic document with digital signature;

(2) Verify the identity of the document signature generator; and

(3) establish secure communication channels with the subscribers.

1.3.5 Applicability

1.3.5.1 Certification applicability

The PublicCA issuance CP defines the assurance class level 1, level 2 and level 3 certification (including certification for signature and encryption)

Equipment or application software certification applies to the Secure Socket Layer (SSL) communication protocol and server application software for dedicated development.

Assurance class applicability is explained below:

Assurance Level	Applicable type of certification	Verification	Applicable scope
Level 1	Natural person, organization,	Verify applicant can really operate the mailing account with	Apply to internet environment with low risk of vicious tempering threat or unable to

Assurance Level	Applicable type of certification	Verification	Applicable scope
	equipment or application software	email	provide comparatively higher assurance class for identification of the subject of certification entity and assure the completeness of the signed document; not applicable to online trading that requires certification. For instance data encryption and identity verification required by email.
Level 2	Natural person, organization, equipment or application software	Applicant is not required to apply at the counter but should provide legal and correct identity certification document of the individual or organization and verified by the RA officer or automatically compared with the reliable database of the system to ensure correctness of applicant information.	Apply to information with possible tempering but no vicious internet tempering environment (information could be intercepted but the probability is not high); not applicable to signature of important documents (documents related to life and high amount trading.) For instance data encryption and identity certification required by small amount ecommerce trading.)
Level 3	Natural person, organization, equipment or application software	Applicant is required to apply at the counter and RA officer verifies correctness of applicant information or use PKI issued assurance class level 3 certification signature	Apply to internet environment with vicious users intercepting or tempering information and risk higher than level 2; delivered information include money for online trading. Applies to identity certification

Assurance Level	Applicable type of certification	Verification	Applicable scope
		to apply and the system automatically compares the information correctness of the applicant.	and data encryption required by e-commerce and financial network trading. The applications including internet banking, internet stock trading, internet tax filing, etc.

Before use and rely on certification service provided by the PublicCA the subscriber and the relying party must carefully read and abide by the CPS and pay attention to the update of the CPS.

1.3.5.2 Certification restrictions

In using the private key the subscriber must select a reliable computer environment and application system to avoid vicious theft or misuse of private key by software and hardware and cause benefit impairment.

Before using certification issued by the PublicCA, the relying party must verify that the type of certification, assurance class and key usage conform to application requirement.

The relying party must appropriately use the individual key and correctly handle the certification attribute information labeled as critical in the certification extension column in accordance with the key usage described in section 6.1.9 recorded in certification.

1.3.5.3 Certification prohibitions

The PublicCA prohibits use of issued certification to following circumstances:

(1) Crime

(2) Military order intelligence and control of nuclear and biochemical weapons

(3) Nuclear energy operation equipment

(4) Aviation and control system

(5) Applicable scope (6) prohibited by law.

1.4 Contact

If you have doubt for the CPS or the subscriber wants to report on missing key, you are recommended to directly contact the PublicCA.

Contact phone: 0800080412。

Mailing address: Public Certification Authority of Chunghwa Telecom, Data Communication Building, 21 Hsinyi Road Section I, Taipei City

Email address: publicca@cht.com.tw。

For other contact information or update of contact information please go to: http://publicCA.hinet.net

2 General provisions

2.1 Obligations and responsibilities

This section explains the rights and obligations of the PublicCA, RA, subscriber and the relying party and accountability of indemnity in the event of occurrence of damages.

删除: PublicCA ,

删除: RA ,

2.1.1 Obligations of the Public Certification Authority of Chunghwa Telecom

(1) Abide by CP and CPS operation.

(2) Identify and verify certification application.

(3) Provide issuance and certification publication service.

(4) Revoke, suspend and resume use of certification.

(5) Issue and publish CRL.

(6) Securely generate private keys of the PublicCA and the CA.

(7) Private key security management.

(8) Use private key in accordance with section 6.1.9.

(9) Support RA for relevant certification registration operation.

(10) Identify and verify personnel of the PublicCA and CA.

2.1.2 Registration authority obligations

Provide certification application service.

(1) Identify and verify certification application.

(2) Notify subscriber and the relying party on the obligations and responsibilities of the PublicCA and the RA.

(3) Notify the subscriber and the relying party to abide by the relevant regulations of the CPS in acquisition or use of certification issued by the PublicCA.

(4) Execute the identification and verification procedures of the RA officer.

(5) Manage the private keys of the RA.

2.1.3 Subscriber obligations

(1) The subscriber must abide by the relevant regulations of the CPS for certification application and verify the correctness of the provided application information.

(2) After PublicCA's approval and issuance of certification application, the subscriber should accept the certification in accordance with section 4.3.

(3) After acquisition of certification issued by PublicCA the subscriber must verify the correctness of the certification information and use the certification in accordance with stipulations in section 1.3.5 and stop using the certification if the information is wrong and notify the RA.

(4) The subscriber should properly store and use his/her private key.

(5) If the subscriber needs to temporarily stop using the certification, resume usage, revoke or re-issue, it is necessary to follow Chapter 4 for handling. In the event of private key information leakage or missing, it is necessary to revoke the certification and speedily notify the RA but the subscriber must still assume legal responsibility of using the certification prior to changes.

(6) The subscriber should exercise prudence in selecting a secure computer environment and a reliable application system and if the computer environment or the application system itself causes damage to benefits

of the relying party the subscriber must assume the responsibility.

(7) If the PublicCA fails to normally operate, the subscriber must speedily seek other ways for completion of legal acts with the other party and must not use abnormal operation of the PublicCA as argument against the other party.

2.1.4 Relying party obligations

(1) In using the PublicCA issued certification or inquiring the PublicCA repository, the relying party must abide by the relevant regulations of the CPS.

(2) In using the PublicCA issued certification, the relying party must first verify the assurance class of the certification to ensure his/her benefits.

(3) In using the PublicCA issued certification, the relying party must verify the recorded certification and the key usage.

(4) In using the PublicCA issued certification, the relying party must first verify the CRL to ensure the certification is valid.

(5) In using the PublicCA issued certification or CRL, the relying party must first inspect the digital signature to ensure that the certification or the CRL is correct.

(6) The relying party must exercise prudence in selecting the secure computer environment and the reliable application system and in the event of damage to the benefits of the relying party or the subscriber due to the computer environment or the application system, the relying party must still assume responsibility.

(7) If the PublicCA fails to normally operate, the relying party must speedily seek other ways for completion of legal acts with the other party and must not use abnormal operation of the PublicCA as argument against

the other party.

(8) In accepting the PublicCA issued certification the relying party is deemed to have understood and consent to the provisions of legal responsibility of the PublicCA and use the certification within the scope specified in section 1.3.5.

2.1.5 Repository obligations

(1) Regularly publish the issued certification, the revoked certification and the CRL in accordance with stipulations in section 2.6.

(2) Publish the latest information of the CPS.

(3) Access control of the Repository must follow stipulations in section 2.6.3.

(4) Publish the results of external auditing.

(5) Maintain the Repository's information accessibility and usability.

2.2 Legal responsibility

2.2.1 The Responsibility of the Public Certification Authority of Chunghwa Telecom

2.2.1.1 Scope of responsibility

The PublicCA shall carry out relevant certification management operations in accordance with the stipulated procedures of Chapter 4 of the CPS.

2.2.1.2 Indemnity exemption

In processing relevant subscriber certification operations the PublicCA

is accountable for indemnity if damage is caused to the subscriber or the relying party for intentional deviation from the CPS or by mistake, violation of relevant laws and regulations and breach of contract between the PublicCA and the subscriber and the relying party. The subscriber should ask for indemnity for damages caused in accordance with relevant contract provisions signed between the PublicCA or the RA and the subscriber; the relying party is entitled to damage indemnity in accordance with relevant laws and regulations. The PublicCA's maximum indemnity for each subscriber or relying party is shown in the table below and if the subscriber or relying party has signed contract with this company with stipulations on the scope of use and trading indemnity restrictions such restrictions must be followed.

Certification assurance class	Maximum indemnity (NT$: dollar)
Level 1	3,000
Level 2	100,000
Level 3	3,000,000

The maximum indemnity is the upper limit of indemnity; actual indemnity should base on the actual damage caused to the subscriber or the relying party.

2.2.1.3 Responsibility exemption

If the subscriber or the relying party does not follow the applicable scope stipulated in section 1.3.5 in using certification, or depart from the CPS, relevant laws and regulations and the contract signed between the PublicCA and the subscriber and the relying party and caused damages and such damages are not attributable to the PublicCA, the subscriber or the relying party shall be liable for damage indemnity.

2.2.1.4 Provisions of exemption

The PublicCA shall not be accountable for legal responsibility if damages are caused by force majeure and any other reasons not attributable to the PublicCA. The PublicCA has clearly set restrictions on the scope for use of certification, henceforth the PublicCA is not accountable for any legal responsibility if damages were caused beyond the scope specified.

For needs of system maintenance, conversion and expansion the PublicCA must publish in advance in the repository to temporarily suspend portions of certification service, and the subscriber or the relying party shall not use this as the reason to ask the PublicCA for indemnity.

For reasons of revoking the certification in accordance with section 4.4.1, the subscriber should apply with the RA for revocation of the certification and after approval of application for revocation of certification the PublicCA shall complete the certification revocation operation within one working day, issue the CRL and publish it in the repository. Before publication of certification revocation, the subscriber shall take appropriate action to minimize effect on the relying party and shall also assume responsibility for use of the said certification.

2.2.2 Responsibility of registration authority

2.2.2.1 Scope of responsibility

The RA shall abide by the procedures stipulated in the CPS and responsible for collection and verification of subscriber identity and relevant certification information registration work and the RA is accountable for legal responsibility caused in the execution of registration work.

The PublicCA issued certification only verifies the identity of the certification entity only to the extent of examination results of the RA officer and does not provide guaranty to the subscriber's financial credit, financial capability, technical capability and reliability.

2.2.2.2 Indemnity exemption

In processing subscriber certification registration operation, the RA shall be accountable for damage indemnity if it intentionally or by mistake does not follow the CPS, relevant laws and regulations and the contract signed between the RA and the subscriber and relevant relying parties and caused damages to the subscriber or the relying party. The subscriber is entitled to ask for damage indemnity in accordance with relevant provisions of the contract signed with the RA; and the relying party is entitled to ask for damage indemnity in accordance with relevant laws and regulations.

2.2.2.3 Responsibility exemption

For reasons attributable to the subscriber and not attributable to the RA, the subscriber or the relying party shall be accountable for damage indemnity for damage caused to the relying party or for any damages occurred.

If the subscriber or the relying party does not follow the CPS, relevant laws and regulations and the contract signed between the RA and the subscriber and the relying party and caused damages or the result of any damages not attributable to the RA, the subscriber or the relying party shall be accountable for damage indemnity.

2.2.2.4 Provisions of exemption

Damages caused for reasons of force majeure and any other reasons not attributable to the RA, the RA is not accountable for any legal responsibility. The RA has clearly specified restrictions on the scope for use of certification and shall not be accountable for legal responsibility for damages caused in use beyond the specified scope.

2.3 Financial responsibility

2.3.1 Financial guaranty

The PublicCA is operated by Chunghwa Telecom Co., Ltd. and latter shall be accountable for former's financial responsibility.

2.3.2 Financial insurance

The PublicCA has not yet bought any insurance for its certification business and will buy insurance in accordance with the competent government department in the future.

2.3.3 Financial auditing

The PublicCA finance is a portion of the entire finance of Chunghwa Telecom Co., Ltd. Chunghwa Telecom Co., Ltd. is a publicly-listed company, and in accordance with article 36 of the Securities Trading Law, the company shall publish the annual financial report within four months after the end of each business year and after filing with the competent government department, certified by the CPA, adopted by the board of directors and approved by the auditors. And within 2 months at end of every half business year, the company shall publish the annual financial report after certified by the CPA, adopted by

the board of directors and approved by the auditors; and within one month at end of the first quarter and the third quarter of every business year, the company shall publish the financial report certified by the CPA.

2.4 Applicable Law and Resolution of Disputes

2.4.1 Applicable law

The interpretation of any agreements signed in accordance with the Certification Practice Statement shall be governed by the relevant laws of the Republic of China.

2.4.2 Divisibility and Survivability

If any section of this certification practice statement becomes invalid, other sections of this CPS will remain effective after removal of the invalid portion, and revision of this CPS is as described in Chapter 8 until revision of this CPS.

2.4.3 Resolution of disputes

In the event of disputes arising between the subscriber or the RA and the PublicCA both parties shall find resolution through consultation in good faith. If litigation is necessary both parties agree to have Taiwan Taipei District Court as the first tribunal for jurisdiction.

2.5 Fees

2.5.1 Certification issuance or extension fee

The fee framework between the PublicCA and the subscriber for certification application, issuance and extension shall be stipulated in

provisions of the sales contract and the subscriber of pertinent provisions should link directly to the repository for inquiry.

2.5.2 Certification inquiry fee

The certification inquiry fee framework shall be stipulated in the relevant provisions of the sales contract and the subscriber of pertinent provisions should link directly to the repository for inquiry.

2.5.3 Certification revocation or status inquiry fee

No charge is required for subscriber download of CRL; online inquiry of the certification status (OCSP function) fee framework shall be stipulated in the relevant provisions of the sales contract and the subscriber can link directly to the repository for inquiry.

2.5.4 Fee return rule

Fees collected by the PublicCA for certification issuance or extension shall be returned to the subscriber if the subscriber certification cannot be used due to the fault by the PublicCA and the subscriber refuses to accept re-issuance of certification after PublicCA investigation for re-issuance. Aside from foregoing circumstances and circumstances stipulated in section 4.9, other fees will not be returned.

2.6 Publication and Repository

2.6.1 Information publication of Public Certification Authority of Chunghwa Telecom

(1) The CPS

(2) CRL

(3) Certification of the PublicCA itself (until expiry of the effective period of certification issued by the public key and the corresponding private key of the certification.)

(4) Issued certification

(5) Privacy protection policy

(6) Latest news related to the PublicCA.

2.6.2 Publication and frequency

(1) The CPS shall be published after approval by the competent department and the CPS shall be revised in accordance with chapter 8 and published in the repository.

(2) The PublicCA issues the CRL once a day and publishes it in the repository.

(3) The certification of the PublicCA itself shall be published in the repository at issuance.

(4) Certification issuance shall be published in the repository at issuance.

2.6.3 Access control

The PublicCA host is installed inside the firewall and cannot be linked directly from outside and the repository is linked to the PublicCA certification management database via its internal firewall to access certification information or download certification. Only authorized personnel of the PublicCA are permitted to manage the repository host.

The PublicCA published information pursuant to section 2.6.1 is mainly for the subscriber and the relying party to use the browser for inquiry. Henceforth, it is open to provide reading and access and is necessary to carry out access control for protection of the security of the repository to ensure accessibility

and usability.

2.6.4 Repository

The PublicCA is responsible for management of the repository and if for reasons normal operation cannot be maintained it will be restored within 2 working days. The repository website is: http://publicCA.hinet.net

2.7 Auditing methods

2.7.1 Auditing frequency

The PublicCA accepts external auditing once a year and irregular internal auditing to ensure operation of the PublicCA genuinely comply with the security regulations and procedures stipulated by the CPS.

2.7.2 Auditor identity and qualifications

The company shall outsource external auditing operation for the PublicCA and assign auditing company that is familiar with PublicCA operation to provide fair and objective auditing service and the auditors should be Certified Information System Audit (CISA) or with equivalent qualifications and experience of auditing a certification organization twice at 4 man-days or relevant experience in information security management auditing, and the PublicCA shall carry out identity identification of the auditors during auditing.

2.7.3 Auditor and auditee relations

The company shall assign a fair third party to carry out auditing of the

PublicCA operation.

2.7.4 Auditing scope

The auditing scope is as follows:

(1) Audits whether the PublicCA complies with the CPS in its operation including the physical environment, personnel procedure control, key control, certification life cycle control, hardware cryptographic module control, and other management and technology auditing.

(2) Verify that the RA complies with the CPS and relevant procedures in its operation.

2.7.5 Counter-measures for auditing results

If auditors find out that the setup and operation of the PublicCA or the RA do not conform to the CPS following actions will be taken:

(1) Records do not conform to circumstances;

(2) Notify the PublicCA about nonconformance;

(3) The PublicCA shall present an improvement plan within 30 days to address the nonconforming items for speedy implementation and listed as items for subsequent auditing tracking. The RA shall be notified for shortcomings for improvement.

2.7.6 Auditing results publishing scope

The PublicCA shall publish information provided by auditors for open explanation.

2.8 Information confidentiality scope

2.8.1 Types of confidential information

Information below generated, received or stored by the PublicCA and the RA are considered confidential.

(1) Operation related private key and passphrase.

(2) Stored information for key sharing.

(3) Subscriber's application information.

(4) Records generated or stored for auditing and tracking.

(5) Auditing records and reports generated by auditors in the course of auditing.

(6) Operation related documents listed as confidential.

(7) The PublicCA and the RA current and retired staff should strictly keep secret of confidential information.

2.8.2 Types of non-confidential information

(1) The issued certification, the revoked certification and the CRL published by the PublicCA repository will not be considered confidential information.

(2) Identification information or information recorded in the certification will not be considered confidential except for special provisions.

2.8.3 Publishing of revoked certification or information temporarily suspended for use

The revoked certification or information temporarily suspended for use shall be published in the PublicCA repository.

2.8.4 Information release under legal procedures

For need of investigation and collection of evidence the Judicial organ, Supervisory organ or Security organ must inquire section 2.8.1 on confidential information in accordance with legal procedures; the PublicCA reserves the right to charge reasonable fees for inquiry by the government organs.

2.8.5 Subscriber demand for information release

The subscriber is entitled to inquire the application information in provision (3) of section 2.8.1; but the PublicCA reserves the right to charge reasonable fees for inquiry by subscribers.

2.8.6 Other information release status

Upon acquisition of subscriber's personal information in operation the PublicCA shall abide by the relevant laws and regulations and shall not disclose the information for protection of subscriber's personal privacy. If the law specifies otherwise the above will not apply.

2.8.7 Privacy protection

The PublicCA processes subscriber's application information in accordance with the law for protection of personal information in computer processing.

2.9 Intellectual property rights

Following items are intellectual properties of the PublicCA:

(1) The PublicCA and the RA public key pairs and key sharing.

(2) Relevant documents written or researched system in implementation of the PublicCA certification management operation.

(3) The PublicCA issued certification and CRL.

(4) The CPS.

The company agrees free download of the CPS from the PublicCA repository or reproduction or distribution in accordance with the copyright law but must ensure complete duplication and expressly state Chunghwa Telecom Co., Ltd. owns the copyright. However, reproduction or distribution of the CPS must not collect fees from other persons and the company shall legally pursue inappropriate usage or infringement on distribution of the CPS.

3. Identification and Verification

3.1 Preliminary registration

3.1.1 Types of naming

The PublicCA uses the X.500 Distinguished Name (DN) for the name of the certification entity for the issued certification.

3.1.2 Naming significance

The certification issued by the PublicCA must conform to relevant naming regulations of the Republic of China with the subject representing its certification entity.

3.1.3 Naming interpretation rule

The naming interpretation rule follows ITU-T X.520 name attribute definition.

3.1.4 Naming uniqueness

The PublicCA's X.500 Distinguished Name is:

C=TW，

O=Chunghwa Telecom Co., Ltd.，

OU=Public Certification Authority

The PublicCA shall use the X.520 standard to define the various naming attributes for assembly to ensure the uniqueness of the X.500 naming space recognized by the PublicCA for name of the subscriber certification entity. The PublicCA subscriber certification entity name permits (but not limited

to) using following X.520 standard defined various naming attributes for assembly:

countryName（abbreviated as C）

stateOrProvinceName（abbreviated as S）

localityName（abbreviated as L）

organizationName（abbreviated as O）

organizationalUnitName（abbreviated as OU）

commonName（abbreivated as CN）

serialNumber

3.1.5 Resolution procedures for naming disputes

When subscribers have identical identification names, the subscriber with early application should have the priority for use. Relevant disputes or arbitration shall not be the obligation of the PublicCA and the subscriber should file application with the competent government department or the court.

If the identification name used by the subscriber has been proved by relevant competent department or department with the right of interpretation that the identification name is owned by other applicant, the said subscriber shall assume relevant legal responsibility and the PublicCA has the right to revoke the subscriber certification.

3.1.6 Trademark identification, verification and role

The certification entity name provided by the subscriber must conform to the trademark law and relevant regulations of the fair trade law of the

Republic of China, but the PublicCA is not responsible for examination whether the subscriber provided certification entity name conforms to the aforementioned regulations; and relevant disputes or arbitration shall not be the obligation of the PublicCA and the subscriber shall handle it in accordance with administrative or judicial relief.

3.1.7 Ways for proving ownership of private keys

The PublicCA shall verify the private keys held by the individual and record in certification as pairs with the public key; it is divided into two ways.

(1) The PublicCA shall generate key pairs on behalf of the subscriber, and at certification issuance the RA shall deliver the subscriber public key to the PublicCA via secure channels, thereby in applying for certification the subscriber does not need to prove holding of private key.

(2) In generating the key pairs, the subscriber then generates the PKCS#10 certification application file and uses the private key for signature and submits the certification application file to the RA at certification application. The RA will use the subscriber public key to verify signature of the certification application file to prove that the subscriber owns a corresponding private key.

3.1.8 Organization identity verification

The organization must provide the RA correct and photocopies of relevant proving documents (such as company update registration card and legal institution registration certification) issued by the competent

government department or legal licensing unit (such as the court) and the photocopies must have the chop of the organization and the chop of the responsible person (the identical chop used at registration of the organization) and the RA would verify the application information provided by the organization.

In applying for level 3 assurance class the organization must authorize an agent to apply at the RA in person and the RA would verify the identity of the agent according to section 3.1.9 on assurance class level 3. If the organization uses assurance class level 3 signature issued by the government Public Key Infrastructure (PKI) for application of certification then the authorized agent is not necessary to apply at the RA in person and the RA system would verify whether its digital signature is valid.

Regarding application information provided by the subscriber the PublicCA has the right to compare the registered information with government provided database or third party database of the relying party in order to verify the identity of the organization.

3.1.9 Personal identity verification

The applicant must provide his/her name, ID number, birth date and present at least one original certified document (such as ID card or passport) with photo for the RA to verify his/her identity.

If the applicant uses the PublicCA certified assurance class level 3 certification signature to apply certification the applicant is not required to verify his/her identity at the RA in person and the RA system would verify his/her digital signature is valid.

The PublicCA has the right to compare the subscriber provided application information with government provided database or registered information of the relying third party database in order to verify his/her identity.

3.1.10 Equipment or application software verification procedure

Regarding computer and telecommunication equipment (such as the router and firewall) or application software (such as the Web Server), the owner of the equipment or application software should apply for certification; identity verification of the organization or the individual should follow stipulations in sections 3.1.8 or 3.1.9.

3.2 Certification key replacement and extension

3.2.1 Certification replacement key

When the usage period of the subscriber private key expires and requires replacement, the subscriber should apply for certification and carry out key replacement operation by identification and verification in accordance with section 3.1.

3.2.2 Certification extension

In applying for certification extension the subscriber should use his/her private key to add signature to the certification application file and submit the certification application file to the RA and latter would use the

subscriber's public key to verify the digital signature of the certification application file to identify the subscriber identity. Expired, suspended and revoked certification must not be extended; and certification can best be extended to the subscriber public key usage period upper limit in accordance with section 6.3.2.2 to ensure the key pair security.

3.3 Certification revocation key replacement

If the subsciber's private key needs replacement because of certification revocation, it is necessary to apply for certification with the PublicCA and the RA would carry out identification and verification of the subscriber in accordance with stipulations in section 3.1.

3.4 Certification revocation

The verification procedures of certification revocation application should be similar to stipulations in sections 3.1.8, 3.1.9 and 3.1.10.

3.5 Certification temporary suspension and resumption for use

In filing application subscriber links to the repository and the RA system would verify his/her identity with the password entered by the subscriber.

4 Operation requirements

4.1 Certification application procedures

To apply for certification follow the steps below:

(1) The certification applicant must fill out the certification application information and agree with the subscriber stipulated provisions.

(2) The certification applicant should deliver the certification application information and relevant certified information to the RA.

(3) If the certification applicant personally generates the key he/she must generate the PKCS#10 certification application file and add signature to the private key and submit the certification application file to the RA in applying for certification.

In applying for certification the applicant must provide correct and complete information. The required information for certification application comprises of mandatory and selective information and only the information listed in the certification format would be recorded in the certification. The RA and the PublicCA would properly store the application information of the applicant in accordance with the CPS.

4.2 Certification issuance procedures

Upon receipt of the certification application information the PublicCA and the RA would carry out relevant examination procedures in accordance with chapter 3 of the CPS as the basis whether or not to agree to issue the certification.

To issue certification follow the steps below:

(1) The RA would pass the examined and approved certification application information to the PublicCA.

(2) Upon receipt of the certification application information from the RA the PublicCA would first verify the relevant RA authorization status and ensure the authorized assurance class and scope and issue certification in accordance with the certification application information passed from the RA.

(3) If the authorized assurance class and scope of RA do not match with the certification application the PublicCA would return relevant error messages to the RA and refuse to proceed with relevant subsequent operations; and if the RA has doubts it should take initiative to consult the PublicCA to ensure the issue is clearly understood.

(4) To ensure security, completeness and undeniability of data transmission between the PublicCA and the RA, the certification application information transmitted via the internet has been encrypted by digital signature and SSL.

(5) The PublicCA has the right to refuse to issue certification to any entity and will not be accountable to the applicant for any damage indemnity.

4.3 Certification acceptance procedures

After completion of certification issuance the PublicCA will notify the applicant to pick up the certification and the subscriber should verify the information in the certification is correct and consistent with the information provided at application, and if errors are found it is necessary to immediately notify the RA for handling or else the subscriber is assumed to have expressed consent to abide by the CPS and rights and obligations of the relevant contracts.

4.4 Certification temporary suspension and revocation

This section mainly describes the circumstances for the need (or necessity) to temporarily suspend or revoke the certification and explains the temporary suspension and revocation procedures.

4.4.1 Reasons for revoking certification

In the event of following circumstances (including but not limited to), the certification subscriber should apply with the RA for revocation of certification:

(1) Loss, theft, tempering and unauthorized disclosure or other damage or usurpation of the private key;
(2) Information carried by the certification that can affect trust of subscriber;
(3) Certification no longer needed for use;

Moreover, the PublicCA has the right to directly revoke certification with notifying the subscriber in advance for one of the following circumstances.

(1) It is sure that portion of information carried by the certification is not true;
(2) It is sure that the certification subscriber signature private key has been stolen for use, fabricated or decrypted;
(3) It is sure that the PublicCA's private key or information system has been stolen for use, fabricated or decrypted and can affect the reliability of certification;
(4) It is sure that the certification has not been issued in accordance with the stipulated procedures of the CPS;
(5) The subscriber has already violated or cannot afford to abide by the rules

or obligations stipulated in the CPS or any other contract and relevant laws and regulations;

(6) In compliance with judicial or prosecutor notification or relevant regulations of the law;

If no certification authority can take up the operation of the PublicCA when latter terminates service, the PublicCA should report to the competent department to arrange to have other certification authority to take up the operation; and if no other certification authority is available to take up the operation the PublicCA will publish in the repository about certification revocation 30 days before termination of service and notify all owners of certification.

4.4.2 Applicants for Certification Revocation

The subscriber, the RA or any legally authorized third party (such as the judicial or prosecutor offices, the authorized agents of organizations and the legal inheritor of the natural person.)

4.4.3 Certification revocation procedures

(1) The certification revocation applicant must submit request for certification revocation in accordance with the operation standards formulated by the RA, and upon receipt of request the RA would proceed with relevant examination procedures and retain all request records pursuant to certification revocation including applicant's name, contact information, reasons for revocation, and time and date for revocation as the basis for subsequent rights and obligations.

(2) After completion of examination operation the RA will deliver the

certification revocation application message to the PublicCA.

(3) Upon receipt of certification revocation application information delivered from the RA the PublicCA will first verify the relevant authorization status of the RA to ensure the authorization assurance class and scope and revoke the certification in accordance with the application delivered by the RA.

(4) If the foregoing examination fails to pass the PublicCA will return relevant error messages to the RA and refuse to proceed with relevant subsequent operations; and if the RA has doubts it should directly contact the PublicCA to ensure that the issue is understood.

(5) To ensure security, completeness and undeniability of data transmission between the PublicCA and the RA, the certification application information transmitted via the internet has been encrypted by digital signature and SSL.

4.4.4 Processing time for certification revocation application

Upon filing certification revocation application by the subscriber, the RA will speedily complete the examination procedures in a working day and after passing the examination the PublicCA will complete the certification revocation operation in one working day.

4.4.5 Reasons for temporary suspension of certification

The subscriber can apply for temporary certification suspension under one of the following circumstances:

(1) Suspicion that the certification key has been stolen for use.

(2) Consideration by subscriber that it is necessary to apply for temporary certification suspension.

4.4.6 Applicant of temporary certification suspension

To be applied by the subscriber.

4.4.7 Temporary certification suspension procedures

The subscriber files application and the RA will verify that the application information is correct and then add digital signature and upload to the PublicCA and latter will immediately terminate the certification. If examination for temporary certification suspension fails to pass the PublicCA will refuse to suspend the certification.

4.4.8 Time for temporary suspension of certification

Upon receipt of temporary suspension of certification by subscriber the RA should complete the examination procedures in one working day and after passing examination the PublicCA should complete temporary suspension procedures in one working day.

In applying for temporary suspension of certification it is unnecessary to specify the period of time for suspension, the PublicCA will set the longest suspension period from application to expiration of the certification.

During the temporary suspension period if the subscriber wants to stop suspension and resume use of certification then the certification would resume as valid.

4.4.9 Certification resumption procedures

In the event the applicant files application for resumption, the RA would

verify the application information is correct, add digital signature and upload to the PublicCA and latter would then immediately resume use of the certification. If application fails to pass examination the PublicCA would refuse to resume use of certification.

4.4.10 CRL issuance frequency

The PublicCA's CRL issuance frequency is once a day. It will be published in the repository for public inspection of the certification status.

4.4.11 CRL inspection regulations

Before using the PublicCA issued certification the relying party should check the PublicCA published CRL or inquire the certification status online to verify the validity of certification.

There are no restrictions on inspection of the CRL by the relying party on the certification information for temporary suspension and revocation published in the repository by the PublicCA. The website is as follows:

http://publicca.hinet.net

4.4.12 Online certification status inquiry service

In using online inquiry of certification status the relying party should check the digital signature of the relevant inquiry results and ensure the source of information is correct and complete.

4.4.13 Online certification status inquiry rules

If the relying party cannot inquire the CRL in accordance with rules in section 4.4.11, then it should use online certification status inquiry service in section 4.4.12 to ensure certification is valid.

4.4.14 Other revocation announcement

Presently there are no other ways for publication of revocation.

4.4.15 Other revocation publication inspection rules

Presently there are no other ways for publication of revocation.

4.4.16 Other special requirements for key decryption

There are no other requirements that are different from sections 4.4.1, 4.4.2 and 4.4.3.

4.5 Security auditing procedures

The PublicCA has kept an audit log for all security related events. The security audit log is a physical mechanism with automatic generation, work record book and paper. All security audit logs are stored for future audit. The security audit log complies with section 4.6.2 for maintenance during the file retention period on events for auditing.

4.5.1 Types of recorded events

- Key generation

- Key generation by the PublicCA is not mandatory restricted to once or generation of key for one time use.
- Private key login and storage
- Login the private key to the system components.
- For ongoing key resumption work the PublicCA retains access to the private key stored.
- Certification registration
- Certification registration application process.
- Revoke certification
- Certification revocation application process.
- Account management
- Add in or delete role and user.
- Revision of user account or role access right.
- Certification format dissection management
- Change of certification format dissection.
- CRL format dissection management
- Change of CRL format dissection.
- Physical access and security of storage area
- Known or suspicion of violation of physical security rules.

- Abnormalities
- Software errors.
- In violation of the CPS.
- Reset the system time clock.

4.5.2 Record file handling frequency

The PublicCA regularly inspects the audit log to interpret the major events. Inspection work includes inspection of all record items to see if there are alert or abnormalities. The audit results should be recorded by documents.

The PublicCA inspects the audit log every two months.

4.5.3 Audit log file retention period

The audit information will be retained on-site for two months in accordance with the management mechanism for retention of information in sections 4.5.4, 4.5.5 and 4.5.6.

When the retention period of the audited information expires, the auditor will remove the information but personnel of other roles must not remove.

4.5.4 Audi log file protection

Current and filed automatic events diary is being securely stored with digital signature to ensure the completeness of the audit log file and only the authorized personnel can read.

4.5.5 Audi log file backup procedures

The electronic audit log should be backup once a month.

(1) The PublicCA should regularly file the events diary.
(2) The PublicCA should store the events diary in a secure place.

4.5.6 Secure auditing system

The PublicCA should keep security audit log for all security related events. The security audit log is a physical mechanism with automatic generation, work record book and paper. All security audit log should be kept for future auditing.

4.5.7 Publication of event entity

When event happens and recorded by the auditing system latter is not necessary to notify the event entity.

4.5.8 Weakness evaluation

The PublicCA should scan the weakness of the certification management system at least once a year and carry out relevant improvement measures.

4.6 Record filing

The PublicCA uses a reliable mechanism for accurately and completely storing the computer information or written information and relevant records of certification operation including:

(1) The important tracking records of the PublicCA generation of key pairs, storage, access, backup and replacement by itself.

(2) Important tracking records of certification application, issuance, revocation and re-issuance.

Aside for provision of tracking or auditing such records can be used as evidence for resolution of disputes. In compliance with foregoing regulations, the RA has the right to ask the applicant or its agent to provide relevant certified documents if needed.

4.6.1 Types of recorded events

The PublicCA has the following recorded filed data:

(1) The PublicCA has the accreditation information of the auditee (assuming it applies.)
(2) The CPS.
(3) Important contracts.
(4) System and equipment configuration setting.
(5) Revision and update of system or configuration settings.
(6) Certification application information.
(7) Revocation application information.
(8) Subscriber identity identification information as stipulated in section 3.1.9.
(9) All issued or published certification.
(10) The PublicCA key replacement records.
(11) All issued or published CRLs.
(12) All audit logs.
(13) Other information or application programs for accreditation and used as evidence for filed contents.
(14) Documents required by the auditor.

4.6.2 Retention period of files

The PublicCA should keep the filed information for at least 10 years. The application programs for processing the filed information should also be maintained for 10 years.

4.6.3 File protection

(1) Users are not permitted to add, revise or delete the filed data.

(2) Through PublicCA authorized procedures the filed data can be moved to another stored medium.

(3) The filed data should be stored in a secure place.

4.6.4 File backup procedures

The PublicCA electronic records should be regularly backup to the storage media by duplication in accordance with the backup procedures and the paper records should be regularly sorted and filed by PublicCA authorized personnel.

4.6.5 Time stamp record requirements

The computer system of the PublicCA would regularly calibrate the time clock to ensure the accurateness and reliability of the date and time information of the electronic records. The filed electronic records (for instance certification, CRL and audit log, etc.) use the standard time after calibration by the system for each recorded time stamp information comprising date and time information and appropriately protected by digital signature and can be used to inspect whether the date and time information have been tempered.

4.6.6 Filed information compilation system

Presently there no filed information compilation system.

4.6.7 Procedures for acquiring and verifying the filed information

In acquiring the filed information of the certification authority relevant personnel must be officially authorized before he/she can take out the filed information.

In verifying the filed information the auditor would carry out the accreditation procedures and written documents must be verified whether the signature and date are true or false.

4.7 Key replacement

The PublicCA private key should be regularly replaced in accordance with stipulations in section 6.3.2. Two months before expiration of the certification the PublicCA should replace the key pairs used for issuing certification. After replacing the key pairs it is necessary to apply for new certification with the PublicCA of Chunghwa Telecom and use the new private key to issue subscriber certification and CRL and re-issue all valid subscriber certification and publish the new certification in the repository for subscribers to download.

The private key of certification subscribers must be regularly replaced in accordance with the stipulations in section 6.3.2 on the usage period of subscriber private key.

4.8 Resumption procedures for key decryption or disaster

4.8.1 Resumption procedures for damage of computer resources, software or information of the PublicCA

The PublicCA has formulated the resumption procedures for damage of computer resources, software and information and concomitantly held rehearsal every year.

If the PublicCA computer equipment was damaged or cannot operate but the signature key has not been damaged, then priority would be given to restoring operation of the PublicCA repository and speedily restore the capability for issuing certification and management.

4.8.2 The Resumption Procedures of Signature Key Certification being revoked by the PublicCA

If the PublicCA signature key certification is revoked it will be published in the repository and notify the relying parties and generate new key pairs in accordance with procedures in section 4.7 and publish the new certification in the repository for download by the subscriber and the relying parties.

4.8.3 The resumption procedures for damage to the signature key of the PublicCA

If the PublicCA signature key was damaged follow the resumption procedures below:

(1)Publish in the repository, notify the subscriber and the relying parties.

(2) Revoke the PublicCA signature key certification and the issued subscriber certification.

(3) Generate new key pairs in accordance with procedures in section 4.7, and publish the new certification in the repository for download by subscribers and the relying parties.

4.8.4 Resumption work for disaster of the security facilities of the PublicCA of Chunghwa Telecom

The PublicCA has formulated resumption procedures after disaster and concomitantly carry out rehearsal every year and in the event of disaster the contingency team will initiate the disaster resumption procedures and give priority to restoring operation of the PublicCA repository and speedily restore the capability of issuing certification and management.

4.9 The PublicCA of Chunghwa Telecom terminates service

To terminate service the PublicCA shall carry out the certification authority service termination procedures in accordance with the relevant regulations of the electronic signature law of the Republic of China. To ensure benefits of the subscriber and the relying party the PublicCA shall proceed accordingly as follows:

(1) The PublicCA shall notify the competent department (Ministry of Economic Affairs) and the subscribers 30 days before the scheduled termination of service;

(2) Before termination of service the PublicCA shall take following measures:

(3) Arrange to have other certification authority to take over the operation for valid certification at termination. And publish in the repository the fact

of terminating service and arranging to have other certification authority to take over its operation and notify the still valid certification subscribers unless they are unable to be notified.

Transfer all the record files during the operation period to the certification authority taking over this operation.

If no certification authority is willing to take over the PublicCA operation, it is then necessary to report to the competent department to arrange to have other certification authority to take over the operation.

If the competent department fails to have arranged another certification authority to take over the operation the PublicCA shall publish in the repository about termination of the still valid certification and notify the certification owners 30 days before termination of service. The PublicCA shall return the certification issuance or extension fees in proportion to the valid period of certification.

If necessary the competent department shall publish revocation of the still valid certification.

5 Control of physical entity, procedures and personnel security

5.1 Physical control

5.1.1 Location and structure of physical entity

The PublicCA computer room is located in the data communication branch office of Chunghwa Telecom. The computer room installation conforms to the standard of storing highly important and sensitive information and is a physical security mechanism with door security, security guard, intrusion detection and video monitoring to prevent unauthorized access to the relevant equipment of the PublicCA.

5.1.2 Physical access

The PublicCA installation shall take appropriate measures to control linking to the PublicCA hardware, software and hardware cryptographic module.

The PublicCA computer room has four levels of door security: the first and the second levels are main entrance and the building security guard throughout the year without rest; the third level is the entrance/exit control system by card readers on each floor; and the fourth level is the finger-printed entrance/exit control system for the computer room personnel and the finger print identification device uses three dimensional finger print sampling to determine the depth and color of the finger print and whether it is a living body to verify door security.

Except for restriction of unauthorized personnel accessing the computer

room with the door security system, the cabinet monitoring system can control opening of the cabinet to prevent unauthorized access to the hardware, software and hardware cryptographic module and relevant equipment.

Portable storage media carrying into the computer room must undergo inspection and verify no computer virus and any vicious software that could damage the PublicCA system.

Non-PublicCA personnel entering the computer room must fill out the entrance/exit record and accompanied by PublicCA personnel throughout the stay.

Before leaving the computer room the PublicCA personnel shall carry out the following inspection work and keep record to prevent entrance into the computer room by unauthorized personnel:

(1) Make sure the equipment normally operates;

(2) Make sure the cabinet doors are closed; and

(3) Make sure the door security system works normally.

5.1.3 Power and air-conditioning

Aside from city power the PublicCA power system is equipped with its own generator（fully loaded with fuel for continuous operation for 6 days）and UPS and provide automatic power switching between city power and the generator and provide at least 6 hours of backup power for the repository to backup information.

The PublicCA has installed the air-conditioning system for constant temperature and humidity to control environmental temperature and humidity to ensure an optimum operating environment for the computer room.

5.1.4 Flood prevention and protection

The PublicCA computer room is installed on the third floor or above in an elevated building on the base and the building is equipped with flood gates and water pumps and there are no major damage records from flooding.

5.1.5 Fire prevention and protection

The PublicCA is equipped with automatic fire detection and warning function and the system can automatically initiate the fire fighting equipment and also installed with manual switch at the main entrances to enable the on-site personnel to operate manually during emergency situations.

5.1.6 Media storage

Aside from keeping the storage media of record audit, files and backup information in places described in section 5.1.1 and have another duplication in a secure place.

5.1.7 Waste material handling

As recorded in section 2.8.1 the PublicCA documents no longer in use shall be scrapped by a paper shredder. Before scrapping any magnetic tape, hard disk, floppy disk, MO and any form of memory must undergo the formatting procedure to remove all stored information. Optical discs shall be physically destroyed.

5.1.8 Backup support from another place

Backup support from another place must be at least 30 km away from the

PublicCA computer room and backup comprises of information and system programs.

5.2 Procedural controls

To ensure secure and reasonable assurance of the system operation procedures, the PublicCA operation procedural controls stipulate the required manpower for each task in terms of the various trusted roles for operation of the PublicCA system and the identification and authentication of each role.

5.2.1 Relying role

The PublicCA must ensure the responsibility of critical PublicCA functions can be appropriately separated and assigned to prevent vicious use of the PublicCA system by certain people without knowing. Each user must implement the required system access for each specified task.

The PublicCA assigns five different PKI personnel roles namely the administrator, officer, auditor, operator and controller to defend against any possible internal attack. The task of each role can be assumed by several persons but each cluster has only one Chief Role to lead the cluster work and the five role task responsibilities are as follows:

The administrator shall be responsible for:

- Installing, setting and maintaining the PublicCA system.
- Setting up and maintaining the system user accounts.
- Generate and backup the PublicCA keys.

The officer shall be responsible for:

- Activating/stopping certification issuance service.
- Activating/stopping the certification revocation service.

The auditor shall be responsible for:

- Inspecting, maintaining and filing the audit logs.
- Implementing or monitoring internal auditing to ensure PublicCA operation follows stipulations of the CPS.

The operator shall be responsible for:

- Everyday operation and maintenance of the system equipment.
- System backup and restoration operation.
- Updating of the storage media.
- Software and hardware update except for the PublicCA certification management system.
- Internet and website maintenance: Set up system security and virus protection mechanism and internet security event detection and notification.
- The controller shall be responsible for:
- The system’s physical security control (computer room door security management, fire and flood prevention and air-conditioning, etc.)

5.2.2 Role assignment

Pursuant to the five trusted roles defined in section 5.2.1 the PublicCA personnel and role assignment shall conform to the following rules:

(1) The trusted roles of the administrator, the officer and the auditor must not overlap but each can concurrently act as operator.

(2) The controller must not concurrently act any of the other four roles.

(3) Under no circumstances must any role implement the self-auditing function and must not permit self-auditing.

5.2.3 Manpower required for each task

In view of operation security of the various working roles the required manpower for each working role is as follows:

(1) Administrator

Require at least 3 qualified personnel.

(2) Officer

Require at least 2 qualified personnel.

(3) Auditor

Require at least 2 qualified personnel.

(4) Operator

Require at least 2 qualified personnel.

(5) Controller

Require at least 2 qualified personnel.

The required manpower for each task is described in the table below:

Task	Administrator	Officer	Auditor	Operator	Controller
Install, set and maintain the PublicCA system	2				1
Set up and maintain the system user accounts	2				1
Generate and backup the PublicCA keys	2		1		1
Activate/stop certification issuance service		2			1
Activate/stop certification revocation service		2			1
Inspect, maintain and file the audit log			1		1
Maintain everyday operation of the system equipment				1	1
System backup support and				1	1

Task	Administrator	Officer	Auditor	Operator	Controller
restoration operation					
Update of storage media				1	1
Software/hardware update except for the PublicCA certification management system				1	1
Internet and website maintenance				1	1

5.2.4 Identification and authentication of each role

Use the IC card to identify and authenticate the administrator, officer and operator and use the central door security system to set restrictions to identify and authenticate the controller.

The PublicCA host operating system account management uses login account number, password and cluster to identify and authenticate the different roles of administrator, officer, auditor and operator.

5.3 Personnel control

5.3.1 Family background, qualifications, experience and security requirements

(1) Security evaluation for personnel recruitment

The selection and use of workers should include following items:

- Personality evaluation.
- Applicant experience evaluation.
- Academic and professional capability and qualifications evaluation.
- Personnel identity verification.
- Personnel integrity evaluation.

(2) Personnel evaluation management

The PublicCA should review the qualifications of the certification operation personnel upon assumption of post to verify his/her reliability and working capability and give appropriate educational training after taking up the job and clearly specify his/her responsibilities in written form, and annually carry out qualifications review to ensure that his/her reliability and working capability have been maintained and if he/she fails to pass the qualifications review then he/she must be transferred to other posts and assign other qualified personnel for the job.

(3) Personnel appointment, removal and transfer management

In the event of changes to personnel appointment and hiring conditions or contracts, particularly personnel departure or termination of the hiring contract must abide by confidentiality stipulations.

(4) Confidentiality stipulations

The working personnel must abide by the confidentiality stipulations and sign the PublicCA contract for preserving business confidentiality. Employees must not disclose business secrets using oral, photocopy, borrowing, assignment, publication of articles or other ways.

5.3.2 Family background inspection procedures

At their early assumption of work the PublicCA must review the qualifications of the various trusted roles in accordance with section 5.2 to ensure their various identity and qualification documents are true.

5.3.3 Educational training requirements

Role	Educational training requirements
Administrator	1. PublicCA security theories and mechanism. 2. Operation procedures for installation, setting and maintenance of the PublicCA system. 3. Operation procedures for setting and maintaining system user accounts. 4. Operation procedures for setting auditing parameters. 5. Operation procedures for generation and backup of PublicCA keys. 6. Procedures for disaster restoration and continuous business operation.

Officer	1. PublicCA security theories and mechanism. 2. Use of PublicCA system software/hardware and operation procedures. 3. Certification issuance operation procedures. 4. Certification revocation operation procedures. 5. Procedures for disaster restoration and continuous business operation.
Auditor	1. PublicCA security theories and mechanism. 2. Use of PublicCA system software/hardware and operation procedures. 3. Operation procedures for generation and backup of PublicCA keys. 4. Procedures for audit log inspection, maintenance and filing. 5. Procedures for disaster restoration and continuous business operation.
Operator	1. Everyday operation and maintenance procedures of the system equipment. 2. System backup support and restoration operation procedures. 3. Storage media updating procedures. 4. Procedures for disaster restoration and continuous business operation. 5. Internet and website maintenance procedures.
Controller	1. Setting physical door security restrictions procedures. 2. Procedures for disaster restoration and continuous business operation.

5.3.4 Re-education training requirements and frequency

Each relevant working personnel of the PublicCA must be familiar with the PublicCA and its relevant working procedures or changes in laws and regulations. In the event of major changes it is necessary to arrange appropriate educational training time within a month to carry out re-training and keep records to adapt to the new working procedures and operation of laws and regulations.

5.3.5 Job transfer frequency and sequence

(1)No concurrent role permitted therefore no job transfer.

(2) After undergoing training and pass examination the operator can be transferred to administrator, officer and auditor work after 2 years.

(3)The administrator, officer and auditor who is not concurrently operator can be transferred to administrator, officer and auditor work one year after working as operator.

5.3.6 Sanctions against unauthorized actions

Relevant personnel of the PublicCA must receive appropriate management and punishment if found to have violated the CP and the CPS or other PublicCA published procedures and in the event of serious offense that caused damages the PublicCA will take legal actions against the offender.

5.3.7 Rules for hiring

The PublicCA hiring security requirements must follow stipulations in section 5.3.

5.3.8 Documentary information provided to personnel

The PublicCA provides CP, CPS and PublicCA system operation manual and documents on the electronic signature law and other implementation details of the Republic of China to relevant PublicCA personnel.

6Technical security control

This chapter describes the PublicCA implemented technical control.

6.1 Key pair generation and installation

6.1.1 Key pair generation

In accordance with stipulation in section 6.2.1 the PublicCA generates key pairs in the cryptographic module using Pseudo Random Number Generator and RSA key algorithm, and the private key generated in the cryptographic module is stored inside to avoid leaking.

The PublicCA key generation shall be carried out under witness of relevant personnel.

6.1.1.1 Generation of subscriber key pairs

Subscriber key pairs can be generated either by the RA or self-generated by the subscriber.

6.1.2 Deliver the private key to the certification subscriber

If the subscriber key is generated by the RA, the RA will forward the subscriber private key with token (for instance the IC card) via the registration window after issuance of certification.

6.1.3 Deliver the subscriber public key to the certification authority

If the RA generates keys for the subscriber the RA will deliver the subscriber public key to the PublicCA via a secure channel.

If the subscriber generates key pairs by itself then the subscriber must use the PKCS# 10 certification application file format to deliver the public key to the RA and latter will inspect that the subscriber really owns the corresponding private key in accordance with stipulations in section 3.1.7 and deliver the subscriber public key to the PublicCA via a secure channel.

Secure channel mentioned in this section refers to the Secure Socket Layer or SSL or any other similar or higher level of data encryption for transmission.

6.1.4 Deliver the certification authority public key to the relying party

The public key certification of the PublicCA itself shall be issued by the PublicCA of Chunghwa Telecom and published in the PublicCA repository to enable subscriber and the relying party for direct download and installation. Before using the PublicCA public key certification the relying party must comply with stipulations of the CPS of the PublicCA of Chunghwa Telecom and obtain the public key of the PublicCA of Chunghwa Telecom via a secure channel or self-issue the certification, and then inspect the signature of the PublicCA public key certification by the Chunghwa Telecom PublicCA to ensure the public key of the public key certification is reliable.

6.1.5 Key length

The PublicCA key length is 2048 bits of the RSA key.

The subscriber key length is 1024 bits of the RSA key.

6.1.6 Public key parameter generation

The RSA algorithm parameter is Null.

6.1.7 Key parameter quality inspection

The PublicCA signature key pairs use ANSI X9.31 algorithm to generate the prime number required by RSA algorithm and the algorithm ensures that the prime number is a Strong Prime.

Subscriber key can generate the prime number inside the IC card or other software/hardware cryptographic module required by RSA algorithm but does not ensure the prime number is a strong prime.

6.1.8 Key generated by software or hardware

The PublicCA and the subscriber use the secure cryptographic module stipulated in section 6.2.1 to generate pseudo random numbers, public key pairs and symmetric keys.

6.1.9 Key usage

The PublicCA signature private key is used for issuing certification and CRL.

If the subscriber key pair is one pair this key pair is used for signature and encryption.

6.2 Private key protection

6.2.1 Cryptographic module standard

The PublicCA uses the FIPS 140-2 Level 3 certified hardware cryptographic module researched by our company.

The storage media for subscriber key pair conforms to ISO 7816 IC card or other carrier.

6.2.2 Multiple control of key sharing

The PublicCA uses the m-out-of-n key sharing for backup and restoration of the PublicCA private key as secure control of key sharing.

Multiple control of subscriber private key will not be stipulated otherwise.

6.2.3 Private key trusteeship

No trusteeship for PublicCA signature private key and the PublicCA will not be responsible for storage of subscriber private key.

6.2.4 Key backup

Backup PublicCA private key in accordance with multiple control of key sharing stipulated in section 6.2.2 and use FIPS 140-2 Level 2 or above to certify IC card for confidential sharing storage media.

6.2.5 Key filing

The PublicCA signature private key shall not be filed but shall file the corresponding private key with certification information in accordance with section 4.6.

6.2.6 Input private key into cryptographic module

The PublicCA shall input the private key into the cryptographic module under one of the following circumstances:

(1) During key generation.

(2) At restoration of key sharing backup. Under such circumstance confidential sharing (m-out-of-n control) is used for PublicCA private key restoration and after restoration of the private key confidential sharing IC card the complete private key will be written into the

cryptographic module.

6.2.7 Private key activation

The PublicCA private key activation is controlled by the IC card cluster using m-out-of-n control and the different usage control IC card cluster is stored by the administrator and officer.

Activation of subscriber private key is not stipulated otherwise.

6.2.8 Private key suspension

The PublicCA private key uses multiple control described in section 6.2.2 to suspend use of private key.

The PublicCA does not provide subscriber private key suspension.

6.2.9 Private key destruction

To avoid the old PublicCA private key being stolen for use and impair the truthfulness of the entire certification the PublicCA shall destroy the private key at expiration of its life cycle, thereby the PublicCA will carry out Zeroization of the old private key stored in the hardware cryptographic module after completion of key update and issuance of new PublicCA certification (refer to section 4.7) to ensure the old PublicCA private key in the hardware cryptographic module is being destroyed.

Aside from destroying the old PublicCA private key in the hardware cryptographic module, the confidential sharing IC card for key backup of the private key shall also carry out physical destruction at the same time during PublicCA key update.

If a key storage module has been permanently stopped to provide service

but is still accessible then all private keys stored in the secure module (including the used or possibly being used) shall be destroyed. After destruction of the key in the cryptographic module, it is necessary to use the key management tool provided by the cryptographic module for inspection to ensure all above-mentioned keys no longer exist.

If a key storage cryptographic module has been permanently stopped for provision of service then all used private keys in the secure module must be erased from the secure module.

Destruction of subscriber private key will not be stipulated otherwise.

6.3 Other key points of key pair management

The subscriber itself shall manage its key pairs and the PublicCA shall not be responsible for storage of subscriber private keys.

6.3.1 Public key filing

The PublicCA shall carry out subscriber certification filing in accordance with stipulations in section 4.6 on secure control of implementing the filing system and shall not carry out filing of subscriber public key.

6.3.2 Usage period of public key and private key

6.3.2.1 Usage period of PublicCA public key and private key

The length of the PublicCA public key and private key is RSA 2048 bits and the usage period of private key is 10 years while the valid period of public key is 20 years.

6.3.2.2 Usage period of subscriber public key and private key

The length of the PublicCA subscriber public key and private key is RSA 1024 bits: The maximum usage period of private key is 5 years while the maximum valid period of the public key is 5 years.

6.4 Protection of activated information

6.4.1 Generation and installation of activated information

After generated by random numbers the activated information shall be written into the cryptographic module and shareholding to the m-out-of-n controlled IC card cluster and to access the activated information in the IC card you must enter your personal identification code into the IC card (hereinafter referred to as the PIN code.)

6.4.2 Protection of activated information

The activated information is being protected by the m-out-of-n controlled IC card cluster and the IC card PIN code is memorized by the storage keeper and must not be written on any media and the new storage keeper will set a new PIN code at transfer of the IC card.

If login failure exceeds three times the IC card would be locked.

6.4.3 Other key points of activated information

The PublicCA private key activated information shall not be filed.

6.5 Computer software and hardware control measures

6.5.1 Specific computer security technical requirements

The PublicCA and its relevant supplementary system shall provide following computer security functions through protective measures of the operating system or by combining the operating system, software and physical entity.

(1) Login with role or identity authentication.

(2) Provide discretionary access control.

(3) Provide secure auditing capability.

(4) Restrictions for various certification service and PKI relying role access control.

6.5.2 Computer security evaluation

The PublicCA certification server uses the Common Criteria EAL 3 certified computer operating system.

6.6 Life cycle technical control

6.6.1 System research control measures

The PublicCA system research must comply with CMMI and ISO 9001standards for quality control.

The PublicCA hardware and software are for dedicated use and can only use security authorized components and must not install and operate irrelevant hardware devices, internet linking or component software.

6.6.2 Security management control measures

First time installation of software in the PublicCA must ensure supplier provides the correct version and not tempered.

The PublicCA will record and control system configuration and any revision and function upgrade and at the same time detect unapproved system software or configuration.

6.6.3 Life cycle security evaluation

Evaluate at least once a year on the risk of the existing key length being decrypted.

6.7 Internet security control measures

The PublicCA host and the internal repository link with the external internet via double firewalls; the external repository is placed in the external service area (Demilitarized Zone or DMZ) outside the external firewall, and link to the internet and provide uninterrupted certification and CRL inquiry service except for necessary maintenance or backup support.

The PublicCA internal repository information (including certification and CRL) is protected by digital signature and automatically delivers from the internal repository to the external repository.

The PublicCA external repository is protected by update of system repairing programs, system weakness scanning, intrusion detection system, firewall system and the filtering router to prevent attack of insulation service and intrusion.

6.8 Cryptographic module security control measures

Refer to sections 6.1 and 6.2.

7 Certification and CRL format dissection

7.1 Certification format dissection

The PublicCA issued certification shall comply with the CPS stipulations.

7.1.1 Version serial number

The PublicCA issues X.509 V3 version certification.

7.1.2 Certification extension column

The certification extension column of the PublicCA issued certification shall comply with RFC3280 stipulations.

7.1.3 Algorithm object identification code

The used algorithm object identification code at signature of the PublicCA issued certification is:

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

(OID：1.2.840.113549.1.1.5)：

At identification generation of the main body key of the PublicCA issued certification the used algorithm object identification code is:

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

(OID:1.2.840.113549.1.1.1)

7.1.4 Ways of Naming

The main body and issuer column values in certification must use X.500 as the sole identification name and the name attributes must comply with RFC 3280 stipulations.

7.1.5 Naming restrictions

No naming restrictions.

7.1.6 CP object identification code

The PublicCA issued certification CP object identification code is 2.16.886.1.100.1.1.2.

7.1.7 Policy restrictions on use of extension column

The PublicCA issued certification does not include policy restrictions on extension column.

7.1.8 Policy qualifiers syntax and semantics

The PublicCA issued certification does not include policy qualifiers.

7.1.9 Semantic handling of critical CP extension column

The CP extension column of the PublicCA issued certification is not remarked as the critical extension column.

7.2 CRL format dissection

7.2.1 Version serial number

The PublicCA issued X.509 v2 version CRL.

7.2.2 CRL extension column

The PublicCA issued CRL shall comply with the RFC 3280 stipulations.

8 CPS Maintenance

8.1 Change procedures

Regularly evaluate the necessity for revision of the CPS to maintain its assurance and the CPS revision will not change the object identification code. Revision methods include adding attached documents and directly revise the CPS.

8.1.1 Change items not notified at change

CPS re-layout will not be notified.

8.1.2 Change items that require notification

8.1.2.1 Change items

Evaluate the extent of effect by the change items on subscriber and the relying party:

(1) For major effect it is necessary to publish in the PublicCA repository for 30 calendar days before revision.

(2) For minor effect it is necessary to publish in the PublicCA repository for 15 calendar days before revision.

8.1.2.2 Notification mechanism

All change items shall be published in the PublicCA repository.

8.1.2.3 Opinion feedback period

Feedback period for opinions on the changed items:

(1) Section 8.1.2.1 (1) for major effect the feedback period is within 15 calendar days from the day of publishing.

(2) Section 8.1.2.1 (2) for minor effect the feedback period is within 7 calendar days from the day of publishing.

8.1.2.4 Opinion handling mechanism

For opinion on change items before the opinion feedback deadline the PublicCA repository will deliver the feedback to the PublicCA and latter will consider the relevant opinions and evaluate the change items.

8.1.2.5 Final publishing period

The CPS published change items shall comply with stipulations in sections 8.1.2.2 and 8.1.2.3 for revision and the publishing period will not be less than 15 calendar days in accordance with stipulations in section 8.1.2.1 until the CPS revision takes effect.

8.2 Publication and notification rules

Within 7 calendar days after revision of the CPS it will be published in the PublicCA repository and the CPS revision effective date will be after publication unless stipulated otherwise.

8.3 CPS review procedures

After approval by the electronic signature law of the competent department of the ministry of economic affairs the CPS shall be published by the PublicCA.

Unless stipulated otherwise, when the CPS revision takes effect the revised CPS should be followed in the event of contradictions between the revised CPS and

the former CPS; and if it is revised by attached documents, the attached documents should be followed in the event of contradictions between the attached documents and the original CPS.