ePKI Root Certification Authority, eCA

Certification Practice Statement

Version 1.1

Chunghwa Telecom Co. Ltd.

2009/01/19

目　　錄

Abstract

Following the provision of items to be clearly stated in the certification practice statement announced and stipulated by the Ministry of Economic Affairs based on the Electronic Signature Law, important matters of the ePKI Root Certification Authority Certification Practice Statements (hereinafter abbreviated as this CPS) are explained as follows:

1.Competent authority approval no: Chin-Shang-Tzu.09800005700

2.Issued certificate:

(1)Types:

The ePKI Root Certification Authority(eCA)，issues two kinds of certificates: The self-signed certificate and cross-certificate.

(2)Assurance Level:

This CPS was stipulated based on the Certification Policy (CP); there are five levels of assurance in this CP which are defined in subsequent Sections.

(3)Applicability:

The self-signed certificate is used to establish the trust anchor of ePKI. The cross-certificate is used to build the trust relationship between interoperable CAs and helps in the certificate path processing within or without a PKI domain.

The subject of the self-signed certificate is eCA itself and like any certificate this self-signed certificate includes the public key of eCA. Anyone can use the self-signed certificate to verify the signature of the cross-certificate and Certification Authority Revocation List (CARL) issued by the eCA.

3.Major Liability

For the Subject CA or relying party by not abiding by the applicability of the certificate utilization provided in this CPS, the eCA will not bear any legal responsibility.

The liability of the eCA to the Subject CA certified by the eCA for damages caused by issuing certificates by the eCA or by using certificates issued by the eCA are subject to this CPS, or contracts or cross-certificate agreements that may be entered into by the certified Subject CA and the eCA.

For any damage or failure caused by force majeure or beyond the reasonable control without the fault or negligence of such party, the eCA shall not bear any legal responsibility

If some certification services have to be suspended temporary because of the system maintenance, alteration and expansion of the eCA, the eCA will announce the information in the repository and notify subscribers. Subscribers or relying parties cannot claim any indemnification based on the above-mentioned reasons to the eCA.

4.Other Important Circumstances

The eCA is responsible for the processing of firsthand certificate applications and revocations. There is no need to set up a Registration Authority (RA) of eCA. The eCA accepts the applications from the subject CAs and authenticates them.

Being fully aware of the different applicability of certificates issued by the eCA according to different assurance levels of the ePKI CP and clearly stating the assurance level under which the Subject CA wishes its own

cross-certificate to be issued when applying for cross-certification from the eCA.

Any CA cross-certified with eCA has to generate the private key by itself.

Any CA that accepting a cross-certificate issued by the eCA implies the confirmation of the correctness of the content of the cross-certificate.

Any CA cross-certified with eCA has to notifying the eCA of any event (such as key compromise or loss) as specified in Section 4.4.1 of this CPS, applying for certificate revocation or suspension in accordance with Section 4.4 of this CPS, and being fully aware that the Subject CA is still liable before the revocation information of its own certificate is published by the eCA.

Relying parties are responsible for ensuring the applicability of certificates issued by the eCA by checking their assurance level approved by the eCA.

Chunghwa Telecom will designate a third party to conduct the eCA external audit operation. The third party shall audit in accordance with the eCA's operation.

1 Introduction

The ePKI Root Certification Authority Certification Practice Statement of Chunghwa Telecom (eCA CPS) is stipulated following the Certificate Policy (CP) for the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI). Complying with the bylaws of the Taiwan Digital Signature Act, the eCA CPS delineates how eCA proceeds according to the Fourth Assurance Level (High) to issue and manage the cross certificates of subject CAs.

According to the regulations of the ePKI CP，eCA is the highest CA in the hierarchical structure of ePKI. , eCA is a trust anchor of ePKI and is stipulated as having the highest assurance level as defined in the ePKI CP. It means that relying parties can trust eCA's certificate directly.

1.1 Applicability

This CPS only applies to the entities related to the community of eCA, such as eCA, Repository, Subject CAs and Relying Parties etc.

The establishment and any modification of eCA CPS may go into effect only after obtaining the permission of Chunghwa Telecom and the eCA.

The terms and provisions of this eCA CPS shall be interpreted and governed by applicable laws. The ROC Government disclaims any liability that may arise from the use of this eCA CPS.

1.2 Identification

This version is 1.1. This CPS was announced on January 19 2009. The latest version of this CPS can be obtained from the following

homepage: http://ePKI.com.tw。

This CPS was stipulated based on the Certification Policy (CP), and the operation of eCA is based on the provision of the CP Assurance Level 4, there are five levels of assurance in this CP which are defined in subsequent Sections. Each level of assurance has an Object Identifier (OID), to be asserted in certificates (not including self-signed certificates) issued by the eCA. The OIDs are registered under the id-tw-gpki arc as follows:

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

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

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

Assurance level	Object identification code	Object identification value
Test level	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
Level 1	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
Level 2	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
Level 3	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}
Level 4	id-cht-ePKI-certpolicy-class4Assurance	{id-cht-ePKI-certpolicy 4}

1.3 Communicability and Applicability

The following summarizes the roles relevant to the administration and operation of the eCA.

(1) eCA

(2) Repository

(3) Subject Certification Authority

(4) Relying Parties

1.3.1 eCA

Operating in accordance with the High Assurance Level defined in the Certificate Policy of ePKI, eCA is the trust anchor of ePKI. Acting as the interface between CAs within and without ePKI, eCA is responsible for carrying out cross-certification: issuing and managing the certificates of Level 1 subordinate CAs' within ePKI as well as the certificates of CAs from without.

The eCA is responsible for the processing of firsthand certificate applications and revocations. There is no need to set up a Registration Authority (RA) of eCA. The eCA accepts the applications from the subject CAs and authenticates them.

1.3.2 Repository

Providing service 7/24, the repository of eCA is where information, such as certificates issued by eCA and CARL (Certification Authority Revocation List), is posted. The web site of the repository is http://ePKI.com.tw.

1.3.3 Subject Certification Authority

CAs, including principal CAs within and any CAs without ePKI, that interoperate with eCA through cross-certification are referred to as subject CAs. To get a grant from eCA for cross-certification, the applicant CA must comply with the requirements of the Assurance level defined in the cited Certificate Policy. Additionally, the applicant CA must have the capabilities to establish and manage the following aspects:

(1) Public Key Infrastructure; (2) digital signatures and certificate issuing technology; (3) the corresponding responsibilities and obligations among CA, RA, and the relying party.

1.3.4 Relying Parties

A relying party refers to an entity who believes the certificate subject name and the connecting relationship of the public key.

The Relying Party is responsible for deciding how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate:

(1) To verify the integrity of a digitally signed message,

(2) To identify the creator of a message,

(3) To establish a confidential communications with the user.

1.3.5 Applicability

1.3.5.1 Usage of Issued Certificates

The eCA issues two kinds of certificates: the self-signed certificate and cross-certificate.

The self-signed certificate is used to establish the trust anchor of ePKI. The cross-certificate is used to build the trust relationship between interoperable CAs and helps in the certificate path processing within or without a PKI domain.

The subject of the self-signed certificate is eCA itself and like any certificate this self-signed certificate includes the

public key of eCA. Anyone can use the self-signed certificate to verify the signature of the cross-certificate and Certification Authority Revocation List (CARL) issued by the eCA.

The subject of a cross-certificate is one CA, which interoperates with the eCA. This kind of CA is termed as Subject CA. The Subject CA will be more than one CA. The Subject CAs will include the Level 1 subordinate CAs within ePKI as well as the CAs from without. There is also a Subject CA's public key in the cross-certificate. Anyone can use the cross-certificate to verify the signature of the certificate and Certification Authority Revocation List (CARL) issued by the eCA.

The certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance level	Applicability
Test level	Only provided for test use and does not bear any legal responsibility on the transmitted data.
Level 1	A rudimentary level of assurance relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter when certificates having higher levels of assurance are unavailable. It is not applicable to on-line transaction that requires certification.

Level 2	A basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. It is not applicable to be signature of important document.
Level 3	A medium level of assurance relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk or involving access to private information where the likelihood of malicious access is substantial.
Level 4	A high level of assurance appropriate for use where the threats to data are high, or the consequences of the failure of security service is high. This may include very high value transactions or high levels of fraud risk.

1.3.5.2 Notifications of Using the Certificate

Relying parties must first obtain the trusted eCA's self-signed certificate or public key via a secure channel as described in section 6.1.4. Then relying parties can use the trusted public key to verify the signature of cross-certificate and CARL that were signed by eCA.

The Relying parties must also make sure the eCA's self-signed certificate or public key is correct and original before verifying the signature of the cross-certificate and CARL that were signed by eCA.

The eCA's cross-certificate will describe which assurance level of the Subject CA and how many levels that the Subject CA can issue cross-certificate to the other CA. And then relying parties can use this information to determine whether they want to trust the certificates issued by a Subject

CA or not. Furthermore, in the content of the eCA's cross-certificate that is issued to a Subject CA which is outside the ePKI, it will have a policy mapping field to describe the certificate policy mapping relation between the eCA and the Subject CA. The relying parties can also be provided with this policy mapping field to determine whether or not they want to trust the certificates issued by a Subject CA.

The Relying parties must read the eCA CPS before they adopt the certification service of the eCA. They should also obey the regulations and pay attention to the modification of this CPS whenever they need.

1.3.5.3 Prohibitions in using the Certificate

(1) Crime.

(2) Control of military orders for nuclear, biological, chemical weapons.

(3) Operation of nuclear equipment.

(4) Control of aviation.

(5) According to applicable laws.

1.4 Contact Details

Contact the Certification Authority if you have any recommendations for the Certificate Practice Statement or if you lost the public key.

The contact phone of this authority: 0800-080412; Address: No. 21, Sec.1, Hsin-Yi Road, Taipei 100; email: service@ePKI.com.tw

Please visit the following website: http://ePKI.com.tw/

2 General Provisions

2.1 Obligations

2.1.1 eCA Obligations

(1) Ensuring that its own operations meet the provisions of the Assurance Level 4 of the ePKI CP,

(2) Establishing the procedures that allow potential Subject CAs to apply for cross-certification,

(3) Identifying and authenticating potential Subject CAs when they apply for cross-certification,

(4) Issuing and publishing certificates as needed,

(5) Revoking certificates as needed,

(6) Issuing and publishing Certification Authority Revocation Lists (CARLs),

(7) Identifying and authenticating the eCA personnel,

(8) Securely generating the eCA private keys,

(9) Ensuring safekeeping of the eCA private keys,

(10) Implementing key rollover of the eCA self-signed certificate as needed, and

(11) Processing application for issuing or revoking cross-certificates from potential Subject CAs.

2.1.2 Subject CA Obligations

(1) Abiding by the provisions of this CPS and the Cross-Certification Agreement between the Subject CA and the eCA and being fully aware that the

Subject CA may be liable for damages otherwise,

(2) Being fully aware of the different applicability of certificates issued by the eCA according to different assurance levels of the ePKI CP and clearly stating the assurance level under which the Subject CA wishes its own cross-certificate to be issued when applying for cross-certification from the eCA,

(3) Submitting valid information for cross-certificate application to the eCA in accordance with the procedure specified in Section 4.1 of this CPS,

(4) Accepting or rejecting its own cross-certificate in accordance with Section 4.3 of this CPS after receiving notification of certificate issuance,

(5) Being fully aware that accepting a cross-certificate issued by the ECA implies the confirmation of the correctness of the content of the cross-certificate, using the certificate in accordance with the procedure specified in Section 1.3.5 of this CPS,

(6) Securely generating its own private keys in accordance with Section 6 of this CPS,

(7) Ensuring safekeeping and proper usage of its own private keys,

(8) Being fully aware that the legal effect of digital signature generated with the private key corresponding to the public key in its own certificate and being fully aware that it should not use the

corresponding private key to generate any digital signature unless the Subject CA confirms that it accepts the certificate, the certificate is still in the validity period, and the certificate is not revoked,

(9) Immediately notifying the eCA of any event (such as key compromise or loss) as specified in Section 4.4.1 of this CPS, applying for certificate revocation or suspension in accordance with Section 4.4 of this CPS, and being fully aware that the Subject CA is still liable before the revocation information of its own certificate is published by the eCA, and

(10) Implementing obligations or liability to other party otherwise in the event that the certification or repository services of the eCA are unavailable, and being fully aware that the event that the certification or repository services of the eCA are unavailable should not be used as an excuse of entering a plea against the other party.

2.1.3 Relying Party Obligations

Relying parties are responsible for:

(1) Abiding by the provisions of this CPS when using certificates issued by the eCA or when seeking information published on the repository of the eCA,

(2) Acquiring the self-signed certificate of the ECA via trusted distribution channel as described in Section

6.1.4 of this CPS,

(3) Ensuring the applicability of certificates issued by the eCA by checking their assurance level approved by the eCA,

(4) Determining the applicability of certificates issued by the ECA by checking their key usage approved by the eCA,

(5) Determining the validity of certificates issued by the eCA by checking the appropriate CARLs published by the eCA,

(6) Verifying the digital signature of certificates and CARLs claimed to be issued by the eCA,

(7) Ensuring that the rely party's computer environment is secure, ensuring that the application system is trustworthy, and being fully aware that the relying party may be liable for damages otherwise,

(8) Implementing obligations or liability to other party otherwise in the event that the certification or repository services of the eCA are unavailable, being fully aware that the event that the certification or repository services of the eCA are unavailable should not be used as an excuse of entering a plea against the other party, and

(9) When the relying party accept the approved certificate issued by the eCA, which means that the relying party has understood and agreed on the terms

of legal responsibility, and will abide by applicable scope of certificate in accordance with the provision provided in section 1.3.5.

2.1.4 Repository Obligations

The repository of the eCA is responsible for:

Regularly publishing the issued certificates, issued CARLs, and other related information in accordance with Section 2.6 of this CPS,

(1) Publishing update information of the ePKI CP and this CPS,

(2) Providing administrative access control mechanisms when needed to protect repository information as described in Section 2.6.3 of this CPS,

(3) Ensuring the availability of the repository.

2.2 Liability

2.2.1 Liability

2.2.1.1 Warranties and Limitations on Warranties

The eCA warrants and promises to operate in accordance with the provisions of the Assurance Level 4 of the ePKI CP and to implement practices to ensure that its certification and repository services, issuance and revocation of certificates and issuance of CARLs are in accordance with this CPS.

2.2.1.2 Disclaimer of Warranties

The eCA assumes no liability whatsoever in relation to the use of certificates issued by the eCA or associated

public-private key pairs for any use other than the uses set out in Section 1.3.5 of this CPS, and subscribers will indemnify the eCA from any such liability.

2.2.1.3 Limitations of Liability

The liability of the eCA to the Subject CA certified by the eCA for damages caused by issuing certificates by the eCA or by using certificates issued by the eCA are subject to this CPS, or contracts or cross-certificate agreements that may be entered into by the certified Subject CA and the eCA.

2.2.1.4 Other Exclusions

The eCA assumes no liability for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to a force majeure.

In the event that the eCA needs to pause all or part of its certification or repository services due to system maintenance, transit, or expansion, the eCA will announce that event on the repository of the eCA and notify Subject CA's; the eCA assumes no liability for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to that event.

In the event that a Subject CA or the governing entity of a Subject CA applies for certificate revocation as set forth in Section 4.4.1 of this CPS, the eCA will accomplish the revocation procedure, which includes validating the application, revoking the certificate, issuing CARLs, and

publishing CARLs no later than 10 working days upon receiving the certificate revocation application and if the application is valid; the Subject CA is still liable, before the revocation information of the certificate is published, for the use of the certificate or its corresponding private key as set forth in this CPS; and it is the responsibility of the Subject CA to take appropriate actions, before the revocation information of the certificate is published, to protect relying parties from damages.

2.3 Financial Responsibility

The ChungHwa Telecom is responsibility for the eCA's operation and financial.

2.3.1 Financial Insurance

The eCA currently has not bought any insurance against the financial responsibility for indemnification. Other aspects of financial responsibility shall be in accordance with applicable law.

2.3.2 Financial Audit

The eCA 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 Interpretation and Enforcement

2.4.1 Choice of Law

Due to the execution of certificate issuance and management operation requirement, the explanation and legality of related agreements signed by eCA shall be processed in accordance with the provision of related laws and regulations.

2.4.2 Severability of Provisions, Survival, Merger

Should it be determined that one section of this CPS is incorrect or invalid, the other section of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in section 8.1.

2.4.3 Dispute Resolution Procedures

If there is dispute between the subscriber and the eCA, both parties shall base on the principle of trust to conduct negotiation and discussion.

If the negotiation fails both parties shall base on the contract to conduct the solution.

2.5 Fees

The eCA is currently being funded centrally; however the eCA reserves the right to charge a fee to each Entity in order to operate the eCA. These fees will only be used to fund operation of the eCA.

In the future, if the eCA changes the fee policy or refund policy, the eCA will update this CPS in accordance with applicable law and publish the new fee mechanism or the new refund procedure.

2.5.1 Certificate Issuance or Renewal Fees

Free of charge.

2.5.2 Certificate Access Fees

Free of charge.

2.5.3 Revocation or Status Information Access Fees

Free of charge.

2.5.4 Fees for Other Services such as Policy Information

Free of charge.

2.5.5 Refund Policy

No fee no refund.

2.6 Publication and Repository

2.6.1 Publication of CA Information

The eCA will publish:

(1) CP,

(2) This CPS,

(3) The CARLs it issues,

(4) The self-signed certificates (Be available at least until all the certificate signed by the corresponding private key of that self-signed certificate expires.),

(5) The cross certificates it issues,

(6) The privacy policy of the eCA,

(7) The latest news about the

2.6.2 Frequency of Publication

The eCA issues a CARL every one day and publishes the CARL in the repository once it is issued.

2.6.3 Access Controls

For the sake of security, the CA host of the eCA will be always kept off-line, and therefore the certificates and CARLs issued by the eCA cannot be sent to the repository directly via a computer network , there exists no any direct or indirect network line between the CA host and the repository. To publish certificates and CARLs to the repository, authorized eCA personnel have to utilize a manual out-of-band transfer via portable media such as a floppy diskette.

The information published in the repository of the eCA as set forth in Section 2.6.1 of this CPS is essential to all Subject CAs and relying parties. Therefore, the public anonymous read access to its information is enabled. Only authorized eCA personnel can update the information stored in the repository. Access controls are set by administrative function and assigned

roles/responsibilities. The eCA will endeavor to maintain the availability of its repository.

2.6.4 Repositories

The eCA operates the repository by itself. In the event that the repository services were suspended due to system damage or any other reason, the eCA is responsible for resuming the repository services in two working days. The URL of the repository is:http://ePKI.com.tw.

2.7 Compliance Audit

2.7.1 Frequency of Compliance Audit

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

2.7.2 Identity/Qualifications of Compliance Auditor

The company shall outsource external auditing operation for the eCA and assign auditing company that is familiar with eCA 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 eCA shall carry out identity identification of the auditors during auditing.

2.7.3 Compliance Auditor’s Relationship to Audited

Party

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

2.7.4 Topics Covered by Compliance Audit

The eCA compliance audit will address:

(1) The eCA operates in accordance with this CPS; and

(2) This CPS outlines, in sufficient detail, the technical, procedural, and personnel practices of the eCA that meet the requirements of the ePKI CP.

2.7.5 Actions Taken as a Result of Deficiency

If deficiencies in the deployment or operation of the eCA with respect to the ePKI CP, this CPS, or Cross-Certification Agreements are found in the audit, the course of actions includes:

(1) The compliance auditor shall note the discrepancy;

(2) The compliance auditor shall notify the eCA of the discrepancy;

The eCA shall present an improvement plan within 30 days to address the nonconforming items for speedy implementation and listed as items for subsequent auditing tracking..

2.7.6 Communication of Results

The eCA will announce the latest audit result in the repository. Except information of the audit result that may cause attack on this authority system, information related to relying parties will be announced.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

Any certificate application information held by the eCA which is not appearing on issued certificates is considered confidential. Both present and former employees are responsible for strictly keeping the confidential information. For the eCA:

(1) All private and secret keys used and handled within the eCA operations are to be kept confidential;

(2) The safekeeping information of the secret shares of the eCA private keys is to be kept confidential;

(3) Any certificate application information held by the eCA will not be released without the prior consent of the subscriber, unless required otherwise by law;

(4) Audit trail records created or retained by the eCA are to be kept confidential;

(5) Audit reports generated during external or internal compliance audits shall not be made available as a whole, except as required by law; and

(6) All classified eCA operational documents and manuals are to be kept confidential.

2.8.2 Types of Information not Considered Confidential

Certificates, Curl’s and revocation/suspension information published in the eCA repository are not considered confidential.

Identification information or other information appearing on certificates is not considered confidential, unless statutes or special agreements so dictate.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

There is no certificate suspension information produced by the eCA since the eCA does not provide certificate suspension service. Certificate revocation information produced is not considered confidential and will be made public in the eCA repository as specified in Section 2.8.2 of this CPS.

2.8.4 Release to Law procedure

In the event that juridical apparatuses, control apparatuses, or security apparatuses need confidential information specified in Section 2.8.1 of this CPS for the purpose of investigation or searching for evidences, the procedure is subject to applicable laws. However, the eCA reserves the right to collect reasonable fees from the inquirer to cover the expense of providing such information.

2.8.5 Disclosure Upon Owner's Request

A Subject CA has the right to inquire certificate application information as specified in item (3) of Section 2.8.1 of this CPS. However, the eCA reserves the right to collect reasonable fees from the inquirer to cover the expense of providing such information.

2.8.6 Other Information Release Circumstances

According to applicable laws.

2.8.7 Privacy Protection

The eCA will protect certificate application information in accordance with “the Privacy Protection Act of Person Data in Computer Processing” of the Republic of China.

2.9 Intellectual Property Rights

The eCA retains all intellectual property rights in and to its own key pairs and their secret shares. A Subject CA retains all intellectual property rights to its own key pairs. However, the eCA retains all intellectual property rights in and to certificates issued by the eCA even though the certificates contain public keys of Subject CAs.

The eCA retains all intellectual property rights to the subject names of its self-signed or self-issued certificates.

The eCA will ensure the correctness of the names of Subject CAs to the best of its capability.

The eCA retains all intellectual property rights to the subject names of its self-signed or self-issued certificates.

The eCA will ensure the correctness of the names of Subject CAs to the best of its capability. However, the eCA shall not be responsible for the dispute resolution of the ownership of the names of Subject CAs. In the event that the registration mark dispute occurs in the name of a Subject CA, the Subject CA should resolve the dispute in accordance with applicable laws and notify the eCA of the result of the dispute resolution in order to protect its own rights.

Chunghwa Telecom Co., Ltd. co-retains all intellectual property rights in and to all documents written for running certificate management service of the eCA.

Chunghwa Telecom Co., Ltd. co-retains all intellectual property rights in and to this CPS. This CPS can be downloaded from the eCA repository for free, and can be, to the extent permitted by the Copyright Act, reproduced or distributed for free provided that the copy is intact. Those who reproduce or distribute this CPS should not charge a fee for this CPS itself and should not restrict the access to this CPS. In no event will the Chunghwa Telecom Co., Ltd. be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any improper usage or distribution of this CPS.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name of the certificate issued by eCA conforms to the Distinguished Name of X.500. The self-signed certificate of eCA and cross-certification certificates among certification authorities use the same type of Distinguished Name.

3.1.2 Need for Names to be Meaningful

The organization names applying for cross-certification should comply with the naming rule of related laws. Meanwhile, names should be able to represent and identify the certification authority.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting various name forms should comply with the Name attribute definition of ITU-T X.520.

3.1.4 Uniqueness of Names

eCA examines the uniqueness of organization names applying for cross-certification. If a duplicate name is found then the applying certification authority is required to change the name.

In favor of international interoperability, the self-signed certificate of eCA uses the following name form:

C = TW，O = Chunghwa Telecom Co., Ltd.，OU = ePKI

Root Certification Authority

Moreover, in the self-signed certificate of eCA the issuer name is identical to the subject name.

3.1.5 Name Claim Dispute Resolution Procedure

The resolution of name claim dispute is the responsibility of. Chunghwa Telecom.

3.1.6 Recognition, Authentication, and Role of Trademarks

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 eCA 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 eCA and the subscriber shall handle it in accordance with administrative or judicial relief.

3.1.7 Method to Prove Possession of Private Key

eCA examines whether the private key of the certification authority in question and the public key in the announcing certificate work in pairs. Using the public key in the PKCS#10 certification request file generated by the certification authority in question to verify the signature in the same file, eCA can insure that the applying certification authority owns the corresponding private key.

3.1.8 Authentication of Organization Identity

The application form for cross-certification submitted by certification authorities should include organization name, locality and representative information that are sufficient to identify the organization. eCA examines the existence of the organization, meanwhile verifies the official document, representative identity and the representative’s authority of representing the organization. The organization representative is required to apply the certificate in person.

For a certificate issued to be used for digitally signing and/or encrypting email messages, the registrant shall prove its ownership of the email address or its authorization from the email address owner to act on the email address owner's behalf. The Subject CA shall take reasonable measures to verify that the registrant controls the email account associated with the email address referenced in the certificate or has been authorized by the email address owner to act on the address owner's behalf;

For a certificate to be used for SSL-enabled servers, the registrant shall prove its ownership of the domain(s) referenced in the certificate or its authorization from the domain owner to act on the owner's behalf. The Subject CA shall take reasonable measures to verify that the registrant has registered the domain(s) referenced in the certificate or has been authorized by the domain owner to act on the owner's behalf; For instance, the Subject CA will verify the ownership of the domain name by checking against an internal or publicly available database.

For a certificate to be used for digitally signing code objects, the registrant shall provide its identity for verification. The Subject CA shall take reasonable measures to verify that the registrant is the same entity referenced in the certificate or has been authorized by the entity referenced in the certificate to act on that entity's behalf.

3.1.9 Authentication of Individual Identity

Not applicable.

3.2 Routine Key Change and Certificate Renewal

3.2.1 Routine Certificates Renewal

Routine key change is the issuance of a new certificate that has the same feature and guaranteed grade as the old certificate. In addition to owning another newly generated public key (paired with a new private key) and a new serial number, the new certificate might be assigned a different valid period.

The private key of eCA itself is 4,096 bits long, valid for 10 years, yet its public key certificate has a validity period of 30 years. eCA will change the key pair and issue a new self-signed certificate if:

(1) Current key pair is expired.

(2) The security of current key pair is dubious. For instance, the private key is suspected or sure to be compromised.

Cross-certification organizations processing the key changes

should apply for new certificates from eCA. The eCA identifies and authenticates the organization applying for cross-certification according to the rules described in section 3.1.8

3.2.2 Certificate Renewal

eCA disallows the renewal of its self-signed certificate and the subordinate cross-certification certificates.

3.3 Rekey after Revocation

After the certificate revocation for certification authorities, the identification and authentication process of the new certificate application follows the rules described in section 3.1 to initialize a registration.

3.4 Revocation Request

The authentication process of certificate revocation requests for cross-certification organizations is the same as the process described in section 3.1.8 and 3.1.9.

3.5 Certificate Suspension and Reactivation

There is no certificate suspension information produced by the eCA since the eCA does not provide certificate suspension and Reactivation

4 Operations Requirement

4.1 Certificate Application

4.1.1 Initiation

(1) Initial application

Cross-certification request form shall be accompanied by the Certification Practice Statement and Certification request file in PKCS#10 format shall be post mailed via formal official document.

If the Certification Authority adopts Certificate Policy other than ePKI-CP, then its complying Certificate Policy shall also be included.

(2) Identification and authentication

Identification and authentication of the applicants shall be performed in accordance with procedures defined in section 3.1.8

(3) Verification

It shall be confirmed that there is no technological incompatibility between applicant Agency and eCA. If ePKI-CP is not adopted, the policy mapping shall be examined. It shall be verified that CPS of applicant Agency complies with its adopting CP. Certification request file in PKCS#10 shall be verified to ensure that the actual cross-certification can be carried out.

4.1.2 Examination

The ePKI Policy Management Committee shall be convened in which the submitted documents together with the eCA verifying summary shall be evaluated. Based on the evaluation, this Committee shall make a determination regarding whether or not to enter into next stage, to demand additional supporting documents, or to reject the request.

4.1.3 Arrangement

An arrangement meeting shall be convened which the applicant agency shall be notified to attend. It shall proceed as follows:

(1) Identification and authentication

Before the commencement of the meeting, the delegate of the applicant agency shall be identified and authenticated in accordance with section 3.1.9.

(2)The terms and conditions to be followed shall be negotiated with the applicant agency.

(3)If the cross-certification is deemed feasible, than it is ratified by signing the Cross-Certification Agreement

(4)Proceed to certificate issuance process.

4.2 Certificate Issuance

Based upon the ratification result of the cross-certification, eCA shall determine whether or not to issue the requested certificate(s).

When the issuance is done, the applicant agency shall be notified

by formal official document with its issued certificate(s) included.

If the request of certificate is rejected, the applicant agency shall be notified by formal official document, with explanation as to why the request was rejected.

A Self-Signed Certificate shall be signed by eCA and shall deliver to the relying parties in accordance with Section 6.1.4.

4.3 Certificate Acceptance

Upon receiving the formal official document for granting the application request, the applicant agency (now Subscriber) shall check the correctness of the content of included certificate(s). If the content is correct, the Subscriber shall sign and send back (in the formal official document) the acceptance document to complete the acceptance procedure. Upon receiving the acceptance document, eCA shall publish the corresponding issued certificate(s) in the depository. If the Subscriber fails to send back the signed acceptance document, it is deemed a refusal of acceptance. In this case, eCA shall revoke the corresponding certificates(s) without further announcement.

If the Subscriber fails to send back the signed acceptance document in thirty calendar days, it is deemed a refusal of acceptance. In this case, eCA shall revoke the corresponding certificates(s) without further announcement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances under which a Certificate may be revoked

The Agency must request for the revocation of its certificate(s), should (but not limited to) any of the following situations occurs:

(1) The corresponding private key of the Agency is suspected or confirmed to be compromised.

(2) The certificate(s) is no longer needed, which may have been due to the termination of the Agency service or termination of the cross-certification between eCA.

In addition, eCA shall revoke the certificate(s) of the Agency without prior approval from the Agency, should any of the following situations occurs:

(1) Incorrectness of any part of the certificates content

(2) Confirmed case of un-authorized use, forge, or compromise of the Agency's private key.

(3) In case of confirmed un-authorized use, forgery, or compromise of the eCA's private key, all of the cross-certificates signed by eCA shall be revoked.

(4) The certificate(s) of Agency is not issued in accordance to this Certification Practice Statement.

(5) The Agency does not operate in accordance with its CPS or Cross-Certification Agreement, or

applicable laws or regulation.

(6) The revocation is requested by the supervising organization of the Agency or is required by laws or regulation.

(7) eCA terminates its services.

If the main information in the certificate needs to be updated, eCA shall review and determine if the certificate should be revoked.

4.4.2 Who can Request Revocation of a Certificate Issued by eCA

Interoperating Agency which requests revocation of its Cross-certificate.

Supervising organization of the Agency

4.4.3 Certificate revocation procedure

4.4.3.1 Initiation

(1) Initial Process

Request shall be brought out via formal official document, with revocation request form filled-in and included.

(2) Identification and authentication

Identification and authentication of the Agency shall be carried out in accordance to section 3.1.8.

(3) Request review

Handed-in documents shall be reviewed to determine the feasibility of the revocation.

(4) Determination

Determine whether to enter next stage, to ask for additional supporting documents, or to notify the Agency via formal official document of the denial of its revocation request. In the case of the denial, explanation shall be enclosed.

4.4.3.2 Certificate revocation

If the revocation request appears to be valid, CA shall revoke the certificate, insert the certificate in CARL, and post the CARL in the CA repository. The Agency and its supervising organization shall be notified of the revocation through formal official document. The certificate status information posted at the depository shall include revoked certificates until its expiration date.

4.4.4 Certificate revocation application processing period

Should any of the situations described in Section 4.4.1 occurs, the Agency shall request for revocation within 10 working days and if possible, before eCA publishes the updated CARL.

4.4.5 Circumstances under which a Certificate may be Suspended

Suspension shall not be provided by eCA.

4.4.6 Who can Request the Suspension of a Certificate

Not applicable.

4.4.7 Certificate temporary suspension procedure

Not applicable.

4.4.8 Certificate temporary suspension processing period and suspension period

Not applicable.

4.4.9 Procedure for Reactivation

Not applicable.

4.4.10 CARL Issuance Frequency

CARLs shall be issued once each day. The updated CARL shall be published in the depository.

4.4.11 CARL Checking Requirements

Before checking CARL published in the depository, the Relying Party should verify the digital signature to confirm the correctness of the CARL. Refer to section 2.6.3 for the conditions necessary for the relying parties to check information that is published in depository.

4.4.12 On-line Revocation / Status Checking

On-line Revocation / Status checking is not provided.

4.4.13 On-line Revocation / Status Checking

Availability

Not applicable.

4.4.14 Other Forms of Revocation Advertisements Available

No other forms of revocation advertisements are provided.

4.4.15 Checking Requirements for Other Forms of Revocation Advertisements

Not applicable.

4.4.16 Special Requirements Related to Key Compromise

In the event of an Agency CA private key compromise, CA shall note in the published CARL that the reason code for revocation of corresponding key is Key Compromise.

4.5 Security Audit Procedures

Audit log files shall be generated for all events relating to the security of the eCA. The security audit logs shall be automatically generated by the system, or manually recorded by a logbook, paper form, or other physical mechanism. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Retention period for archive, Section 4.6.2.

4.5.1 Types of Events Recorded

- Security Audit
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Identification and Authentication
- Successful and unsuccessful attempts to assume a role
- Change in the value of maximum authentication attempts
- Maximum number of unsuccessful authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from password to biometrics
- Key Generation
- Whenever eCA generates a key.
- Private Key Load and Storage
- The loading of Component private keys
- All key recovery works, and the access of the private key stored in the eCA
- Trusted Public Key Entry, Deletion and Storage
- All changes to the trusted public keys, including additions and deletions
- Private Key Export
- The export of private keys (keys used for a single session or message are excluded)
- Certificate Registration
- All certificate requests and processes
- Certificate Revocation
- All certificate revocation requests and the processes
- Certificate Status Change Approval
- The approval or rejection of a certificate status change request
- eCA Configuration
- Any security-relevant changes to the configuration of the eCA

- Account Administration
- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified
- Certificate Profile Management
- All changes to the certificate profile
- Certificate Revocation List Profile Management
- All changes to the certificate revocation list profile
- Miscellaneous
- Installation of the Operating System
- Installation of the eCA
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules
- System Startup
- Logon Attempts to eCA Apps
- Receipt of Hardware / Software
- Attempts to set passwords
- Attempts to modify passwords
- Backing up eCA internal database
- Restoring eCA internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any material to a repository
- Access to FBCA or Agency CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Transmission of token
- Zero value of token
- Rekey of eCA or Agency CA
- Configuration changes to the eCA server involving:
- Hardware
- Software
- Operating System
- Patches
- Security Profiles
- Physical Access/Site Security
- Personnel Access to room housing eCA
- Access to the FBCA or Agency CA server
- Known or suspected violations of physical security

- Anomalies
- Software Error conditions
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure
- Obvious and significant network service or access failures
- Violations of Certificate Policy
- Violations of Certification Practice Statement
- Resetting Operating System clock

4.5.2 Frequency of Processing Data

eCA shall review audit logs once every month to keep track all significant events. Such reviews involve verifying that the log has not been tampered with, inspecting all log entries, and investigating any alerts or irregularities in the logs.

Actions taken as a result of these reviews shall be documented.

4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for two months as well as being retained in accordance with sections 4.5.4、4.5.5、4.5.6 and 4.6.

The removal of the expired audit logs of the eCA system shall be performed by no other parties than the auditors.

4.5.4 Protection of Security Audit Data

Current and archived audit data shall be protected by digital

signing and encryption technologies and shall be stored in CD-R or other non-modifiable storage media.

Private keys used to sign event log shall not be used for any other purpose. Use of Private keys of audit system for any other purpose is strictly prohibited. Audit system shall not reveal private keys.

Manual audit logs shall be moved to a safe, secure storage location.

4.5.5 Security Audit Data Backup Procedures

Electronic audit logs and audit summaries shall be backed up monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

eCA shall periodically back up the event logs: audit system shall automatically archive the audit trail data daily, weekly and monthly.

eCA shall store audit logs in a safe location.

4.5.6 Security Audit Collection System (Internal vs. External)

Audit processes shall be invoked at eCA system startup, and cease only at eCA system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the eCA shall temporarily stop issuing certificates until the problem is remedied.

4.5.7 Notification to Event-Causing Subject

When an event was audited, the audit system does not need to provide notice to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

- Vulnerability Assessment on the operation systems.
- Vulnerability Assessment on the physical facilities.
- Vulnerability Assessment on the certification authority systems.
- Vulnerability Assessment on the network

4.6 Records Archival

4.6.1 Types of Events Archived

- eCA accreditation record
- Certification Practice Statement
- Cross-certification agreement
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Documentation of receipt and acceptance of certificates
- All certificates issued or published
- Record of FBCA or Agency CA Re-key
- All CARLs and CRLs issued and/or published
- All Audit Logs
- Other data or applications to verify archive contents
- Documentation required by compliance auditors
- Subscriber identity Authentication data as per Section 3.1.8.

4.6.2 Retention Period for Archive

The retention period for archive data in eCA is 20 years. Applications required processing the archive data shall also be

maintained for 20 years.

4.6.3 Protection of Archive

It is not permitted to write to, modify, or delete the archive

eCA may move archived records to another storage medium and shall provide proper protection with level of assurance not lower than the original one.

Archive media shall be stored in a safe, secure storage facility.

4.6.4 Archive Backup Procedures

The backup of archive data shall be stored in off-site support center (Refer to section 5.1.8)

4.6.5 Requirements for Time-Stamping of Records

Electronic archive data (such as certificates, Certification Authority Revocation Lists and audit data, etc.) shall be time-stamped and protected by proper digital signatures so that the integrity of the time-stamps can be verified. However the time-stamps on these archive data are not electronic time-stamps provided by trusted third-party. Rather, they are obtained from the clock of computer operation system. The system clocks of all the computers of eCA shall be periodically adjusted to ensure the precision and reliability. The paper archive documentation shall also be dated, and even time-stamped if necessary. The time and date on the paper documentation shall not be altered unless the modification is acknowledged and signed by the auditors.

4.6.6 Archive Collection System (Internal or External)

eCA does not have an archive collection system.

4.6.7 Procedures to Obtain and Verify Archive Information

Archive information may be obtained upon the receipt of formal authorization of request in-writing. The auditors are in charge of verifying the archive information. In the case of paper documentation, the authenticity of the dates and signatures shall be verified, whereas the digital signature of the electronic archive information will be verified.

4.7 Key Changeover

The eCA's signing key shall be changed no later than 3 months prior to the expiration date of its self-signed certificate. A new self-signed eCA certificate shall be issued at the same time. New self-signed certificate shall be delivered to the relying parties in accordance with section 6.1.4.

Cross-certified organizations shall change their signing keys no later than 2 months prior to the expiration date of their certificates and shall request (in accordance with section 4.1) new certificates from eCA after key changeover is done.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and/or Data

are Corrupted

eCA shall define recovery procedures used if eCA computing resources, software, and/or date are corrupted. Recovery drill will be practiced every year. If eCA equipment is damaged or rendered inoperative, but the eCA signature keys are not destroyed, eCA operation shall be reestablished as quickly as possible, giving priority to the operation of eCA repository.

4.8.2 Signature Keys are Revoked

eCA shall define recovery procedures used if the eCA signature keys are revoked. Recovery drill will be practiced every year.

4.8.3 eCA Signature Keys are Compromised

eCA shall define recovery procedures used if the eCA signature keys are compromised. Recovery drill will be practiced every year.

4.8.4 Secure Facility after a Natural or Other Type of Disaster

eCA shall practice the disaster recovery drill of the secure facility every year.

4.9 CA Termination

In the event of termination of the eCA operation, it will follow the procedure defined by Electronic Signatures Act to minimize the impact on the subordinate CA's and the subscribers in the event of termination, eCA will:

Notify the cross-certificating organizations and publish the announcement in the depository 3 month before the proposed termination date.

Revoke any un-revoked or not expired certificates upon termination, and safe-keep and consign record archive following the regulation defined in Electronic Signatures Act.

5 Non-Technical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The eCA facility is located in the housing of Chunghwa Telecom Data Communication Branch. The construction of the facility housing is consistent with facilities used to house high value, sensitive information. Combined with other physical security protection mechanisms including guards, video monitoring and intrusion sensors it provides robust protection against unauthorized access to the eCA equipments.

5.1.2 Physical Access

The physical access control of the eCA meets the level 4 assurances defined in the ePKI CP. There are four guarding levels in the eCA facility housing. The first and second levels are 24 hours entry guards and building guards. The third level using IC card technology performs the building story access control. The forth level is a fingerprint access control system that uses a 3D sampling technology and is capable of detecting the tint, penetration and live state.

The physical access control system of the eCA is able to protect the facilities from unauthorized access. The computer rack is able to prevent any unauthorized access to any hardware, software, or hardware secure module in the eCA.

Any portable storage device brought to the facility housing

shall be checked without computer software virus and any other software that may damage the eCA system.

Under certain circumstances, unauthorized persons may need to be in the facilities housing. This access can only be performed when an authorized person is presented and all actions taken by the unauthorized person shall be recorded.

The authorized person needs to perform the following checks after the unauthorized persons is left the facilities housing

(1) Check the operation of system equipment

(2) Lock the computer rack

(3) Check the operation guarding system

5.1.3 Electrical Power and Air Conditioning

In addition to commercial power, the power system of the eCA has backup capability and is provided with Uninterrupted Power System. The switch between commercial power system and backup power system is automatic and the power shall be sufficient for a minimum of six hours operation to backup the process data.

The eCA facilities housing has an automatic temperature and a humidity control system to provide a proper environment for the operation of the eCA.

5.1.4 Flood Prevention and Protection

The eCA facilities housing is placed in a building without any flooding damage history. The building has water gate and water pump protection and the story used for the eCA equipment

is higher than third story.

5.1.5 Fire Prevention and Protection

The eCA facilities housing has an automatic fire prevention and protection system and every entry provides a switch that allows person in emergency situation manually enable the fire prevention and protection system.

5.1.6 Media Storage

The data of audit, archive, and backup shall be stored in the facilities housing at least one year. After one year, the data shall be moved to the off-site backup location that is separated from the eCA system.

5.1.7 Waste Disposal

When the secret information and documents of the eCA described in section 2.8.1 become useless all paper shall be processed by a paper cutting machine; tapes, hard disks, disks, MO and other types of memory shall be formatted to erase all information and than physically destroyed.

5.1.8 Off-site Backup

The off-site backup location is in Taoyuan, 30 km away from the eCA facilities housing. The information including system programs and data shall be duplicated at lease once per week. Modified data shall be duplicated within 24 hours. The backup site has physical and procedural controls commensurate to that of the operational eCA.

5.2 Procedural Controls

In order to protect the security of the eCA operations, the eCA uses procedural controls to define the roles of operators, the number of persons required per task, and the identification and the authentication for each role.

5.2.1 Trusted Roles

In order to properly separate the duty of each operation and to prevent the damage caused by internal operations, the execution of every operation performed in the eCA is clearly defined according to operator roles. There are five trusted roles defined in the eCA including administrator, officer, auditor, operator, and controller. Each role is administrated according to section 5.3 to prevent the damage cause by internal operators. Every trusted role can be assigned to one individual or a group and one of that groups should be assigned as chief role. The job for each role is assigned as the followings.

(1)Administrator: authorized to install, configure, and maintain the eCA; establish and maintain user accounts; configure profiles and audit parameters; and generate as well as backup component keys.

(2)Officer: authorized to request or approve certificates or certificate revocations.

(3)Auditor: authorized to review, maintain, and archive audit logs; perform or oversee internal compliance audits to ensure that the eCA is operating in

accordance with its CPS

(4)Operator: authorized to execute the routine operation of the eCA equipment and operations such as system backups and recovery or changing recording media; Update software except the eCA system programs; maintain the networks and Web servers including building an antivirus system capable of detecting and reporting the network security events.

(5)Controller: authorized to execute the physical controls of the eCA facilities. (System access controls, air condition, flood, and fire prevention…)

5.2.2 Roles Assignments

The trusted roles as defined in section 5.2.1 must comply with the following roles

(1)Individual may assume only one of the Administrator, Officer, and Auditor roles, but the individual may assume the operator role.

(2)The controller may not assume other roles.

(3)No individual may execute the self-audit function

5.2.3 Number of Persons Required Per Task

According to the security requirements, the number of each trusted role is assigned as the following:

(1) Administrator:at least 3 qualified individuals

(2) Officer: at least 3 qualified individuals

(3) Auditor: at least 2 qualified individuals

(4) Operator: at least 2 qualified individuals

(5) Controller:at least 2 qualified individuals

The number of each assignment is given as the following:

Assignments	Administrator	Officer	Auditor	Operator	Controller
Installation, configuration, and maintenance of the eCA;	2				1
Establishing and maintaining the eCA user accounts	2				1
Configuring audit parameters	2				1
Generating and backing up the eCA keys	2		1		2
Issuing certificates		2			1
Revoking certificates		2			1
Publishing CARL		1			1
Reviewing, maintaining, and archiving audit logs			1		1
Daily routine operation				1	1
System backing up and recovery				1	1
Changing recording media				1	1
Software and hardware update except the eCA system				1	1
Maintaining Network and Web server				1	1
Configuring physical controls					2

5.2.4 Identification and Authentication for Each Role

The eCA utilizes system account management functions and IC cards to identify and authenticate administrator, office, auditor, operator, and controller.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

(1) The evaluation items of security requirements

- Personality
- Experiences
- Academic and professional qualifications
- Personal Identification
- Trustworthiness

(2) The management of trusted roles

All eCA operators shall be identified and authenticated before being permitted to perform any action. All operators shall receive comprehensive training and sign a document to accept the responsibility of performing duties. All operators shall be evaluated every year, and if individual cannot pass the evaluation, he/she should be replaced by a qualified individual.

(3) The shift of eCA operators

The hiring or the changes of employee contract,

especially personal quit or contract terminated the personal shall obey the role of keeping the confidential information of the eCA.

(4) The responsibility of keeping confidential information All eCA operators shall sign a contract to keep the information about the eCA as confidential and the confidential information cannot be revealed through copy, publish, or other methods.

5.3.2 Background Check Procedures

The eCA shall check the requirements and necessary documents to identify the trusted roles defined in Section 5.2.1.

5.3.3 Training Requirements

Trusted Roles	Training Requirements
Administrator	eCA authorization Installation, configuration, and maintenance of the eCA Establishing and maintaining the procedure of cross certification Establish the procedure of configuring audit parameters The procedure of generation and backup component keys The procedure of disaster recovery and daily maintenance
Officer	eCA authorization The operations of both eCA software and hardware The procedure of issuing certifications The procedure of revoking of certifications The procedure of disaster recovery and daily maintenance
Auditor	eCA authorization The operations of both eCA software and hardware

Trusted Roles	Training Requirements
	The procedure of generation and backup component keys Reviewing, maintaining, and archiving audit logs The procedure of disaster recovery and daily maintenance
Operator	eCA authorization The routine operations The procedure of changing recording media The procedure of disaster recovery and daily maintenance The maintenance of Web Services
Controller	The procedure of configuring the physical controls The procedure of disaster recovery and daily maintenance

5.3.4 Retraining Frequency and Requirements

All operators shall aware of the changes of the eCA software or hardware upgrade, routine procedure, CP, or CPS. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented to insure that all operators understand the changes.

5.3.5 Job Rotation Frequency and Sequence

There is at least one year needed before an administrator can be shifted to be an operator or an auditor.

There is at least one year needed before an officer can be shifted to be an administrator or an auditor.

There is at least one year needed before an auditor can be shifted to be an administrator or an officer.

After a properly training and two years experiences, an operator can have the qualification to be an operator, an

administrator, or an auditor.

5.3.6 Sanctions for Unauthorized Actions

The eCA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving eCA or its repository not authorized in this CP, the eCA CPS, or other procedures published by the eCA Operational Authority.

5.3.7 Contracting Personnel Requirements

The safety requirement of recruiting personnel of this authority shall base on the provision of section 5.3.

5.3.8 Documentation Supplied to Personnel

The eCA shall make available to its CA and RA personnel the certificate policies it supports, relevant parts of the CPS, and any relevant statutes, policies or contracts.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

According to section, 6.2.1, eCA generates key pairs using RSA algorithm within the hardware security module via True Random Number Generator; private keys are generated within the hardware security module and they are not distributed at all.

eCA Key generation is witnessed by those related personnel who also sign the (eCA) Public Key Initiation Witness document; this document records the public key pairs generated. This public key is distributed via the trusted channels.

A CA which is cross-certified with eCA must generate key pairs according to its Certificate Policy.

While issuing cross certificates to its cross-certified CAs, eCA checks the public key in each certificate request file to ensure that each CA's public key is unique.

6.1.2 Private Key Delivery to Cross-certified CAs

Any CA cross-certified with eCA has to generate the private key by itself. Therefore, eCA does not need to deliver private keys to any cross-certified CA.

6.1.3 Public Key Delivery to eCA

A cross-certified CA will send its PKCS#10 certificate request when it requests for cross certification with eCA.

6.1.4 eCA Public Key Delivery to Relying Parties

eCA self-signed certificate contains its public key. There are several secure distribution channels as follows.

(1)After eCA has issued a cross certificate to a CA, it will deliver this cross certificate along with the eCA self-signed certificate or public key to this CA. This CA stores eCA self-signed certificate or public key into the token (such as IC card, etc). This CA distributes such token securely to the certificate users or relying party.

(2)eCA self-signed certificate is stored in the build-in reliable software issued by trusted third party. Certificate users obtain this software via the secure channel (for example, purchase software installation CD-DOM from reliable distributors). After the installation, eCA self-signed certificate is obtained by the certificate users simultaneously.

(3)eCA self-signed public key certificate stores in CD-ROMs with large volume of circulation; certificate users obtain these CD-ROMs via secure channels, at the same time, they will obtain the eCA self-signed certificate.

(4)While eCA is activated, its public key will be announced; at the same time, related personnel will sign eCA public key witness document and deliver it

to the media for announcement. Relying party can compare the eCA public key announced by the media with the one contained in the eCA self-signed public key certificate downloaded from Internet.

6.1.5 Key Sizes

eCA adapts 4096-bit RSA public keys pairs and SHA-1 hash function to issue certificates. A cross-certified CA has to follow its certificate policy to choose a proper key size. eCA will exam whether this CA has chosen an appropriate key size before it issues a cross certificate to this CA.

6.1.6 Public Key Parameters Generation

The public key parameter of the RSA algorithm is Null.

6.1.7 Parameter Quality Checking

eCA adapts ANSI X9.31 algorithm to generate the prime numbers used in the RSA algorithms. This method can guarantee such generated prime numbers are strong prime.

A cross-certified CA has to proceed key parameters quality checking depending on the algorithm it chooses.

6.1.8 Hardware/Software Key Generation

eCA adapts hardware cryptographic modules to generate random numbers, public keys and symmetric keys.

A Cross-certified CA has to follow the stipulations from its certificate policy to choose appropriate software and/or hardware to generate keys. Before issuing a cross certificate, eCA will

examine whether the software and software chosen by this CA is appropriate.

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

The private key corresponding to the eCA self-signed certificate can only be used for issuing certificates and ARL. eCA self-signed certificate does not contain the KeyUsage extension field.

Cross certificates issued by eCA set two key usage bits: cRLSign and CertSign , in the KeyUsage extension field.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

According to the certificate policy, eCA uses hardware secure modules with the assurance level 3.

A Cross certified CA has to follow the stipulations from its certificate policy to choose an appropriate cryptographic module. Before issuing a cross certificate, eCA will check whether the assurance level of the cryptographic module chosen from this CA is appropriate.

6.2.2 Private Key (n out of m) Multi-person Control

eCA private key multi-person control adapts the m-out-of-n LaGrange Polynomial Interpolation. It is a perfect secret sharing method which can be used for private key splitting and recovering. Adapting such method can guarantees the highest assurance level

for eCA private key multi-person control; therefore it can be used for the private key activation method (also refer to section 6.2.7).

If eCA is about to issue a private key which is used for CA's digital signature generation with assurance level 3 or 4 to a CA, it has to follow its certificate policy to adapt multi-person procedure. Before issuing a cross certificate, eCA examines whether this CA has adapted an appropriate Multi-Person control.

6.2.3 Private Key Escrow

The eCA private key used for digital signature generation cannot be escrowed. eCA is not responsible for managing any private key used for signature from any cross-certified CA.

6.2.4 Private Key Backup

According to section 6.2.2, eCA adapts the private key multi-person control to backup the private key. It also uses highly secure IC cards to store secret sharing.

A cross-certified CA has o follow stipulations from its certificate policy to choose an appropriate private key backup method. Before issuing a cross certificate, eCA has to examine whether the private key backup method chosen by this CA is appropriate.

eCA does not responsible for managing private key backups for any cross-certified CA.

6.2.5 Private Key Archival

The eCA private key for digital signature cannot be archived. eCA does not archive any CA's private key used for digital

signature.

6.2.6 Private Key Entry into Cryptographic Module

Only when eCA is backing up keys, it can import private keys into cryptographic modules.

If a cross-certified CA needs to import a private key into cryptographic modules, then it has to follow its certificate policy to choose an appropriate private key importing method. Before issuing a cross certificate, eCA examines whether the private key import method chosen by this CA is appropriate.

6.2.7 Method of Activating Private Key

eCA RSA private key activation is controlled via m-out-of-n controlling IC cards; controlling IC cards with different usages are managed by managers and issuers separately.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate private key activation method. Before issuing a cross certificate, eCA examines whether the private key activation method chosen by this CA is appropriate.

6.2.8 Method of Deactivating Private Key

As eCA adapts offline operating mode, normally eCA key pairs will be at deactivation state in order to avoid any illegal use of its private key.

Once completing the certificate issuing and relative management operations, eCA adapts m-out-of-n method to suspend its private key.

A cross-certified CA has to follow the stipulations from its certificate policies to choose an appropriate private key suspension method. Before issuing a cross certificate, eCA examines whether this CA has chosen an appropriate private key suspension method.

6.2.9 Method of Destroying Private Key

In order to prevent eCA old private key from being stolen, which will influence the correctness of issued certificates, eCA private key will be destroyed once it reached its complete life cycle. Therefore, after the completion of eCA key renewal and new certificate issuing processes, eCA will implement the Zeroization process in the memory in order to destroy the old private key stored in the hardware cryptographic module. At the same time, old private key splits are destroyed physically.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate private key destroying method. Before issuing a cross certificate, eCA examines whether the private key destroying method chosen by this CA is appropriate.

6.3 Other Aspects of Key Pair Management for Cross-certified CAs

Cross-certified CAs has to manage their own key pairs; eCA is not responsible for private keys of any cross-certified CA.

6.3.1 Public Key Archival

eCA will proceed the certificates archival, and also follow regulations from section 4.6 to perform the security control for archival systems. There is no other procedure for public key archival, as certificates archival can replace the public key archival.

6.3.2 Usage Periods for the Public and Private Keys

6.3.2.1 Usage Periods for eCA's Public Key and Private Key

RSA Key sizes for both eCA's public key and private key are 4096 bits. Public key certificates usage period is at most 30 years; private key usage period is at most 10 years.

6.3.2.2 Usage Periods for Cross-certified CA's Public Key and Private Key

(1) RSA 2048 bits: public key certificates usage periods are at most 20 years; private keys usage periods are at most 10 years.

(2) RSA 1024 bits: public key certificates usage periods are at most 10 years; private keys usage periods are at most 5 years.

The usage period of the cross certificates issued to cross-certified CAs, plus the eCA private key (used for digital signature) usage period, cannot exceed the life usage period of eCA self-signed certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

eCA activation data is generated by hardware cryptographic module then stored in the m-out-of-n controlled IC cards. The activation data within the IC cards will be accessed directly by the built-in card readers in hardware cryptographic module; the IC cards person identification number (abbreviated as PIN) will be input directly from the built-in keyboard in the hardware cryptographic module.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate data activation method. Before issuing a cross certificate, eCA examines whether this data activation method chosen by this CA is appropriate.

6.4.2 Activation Data Protection

eCA activation data is protected by the m-out-of-n control IC cards; IC card PINs are kept safe by the managers. It does not allow keeping PIN records on any media. If the number of failed login exceeds 3 times, this IC card is locked. When IC card is handed over, the new manager has to reset a new PIN.

A cross-certified CA has to follow the stipulations from its certificate policy to choose an appropriate activation data protection method. Before issuing a cross certificate, eCA examines whether this method of activation data protection method is appropriate.

6.4.3 Other Aspects of Activation Data

The activated information of private key of this authority will not be archived.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Through the operating systems, or combining operating system software and physical entity protection measures, eCA and related auxiliary systems provide the following security control functions:

- To login with authentication
- To provide self-discretionary access control
- To provide security audit capability
- To restrict access control from certificate services and trust roles
- To process trust role and trust identity authentication
- To ensure the security of communication and database by adapting cryptographic technology
- To process the secure and reliable channel for trust role and relative identity authentication.
- To process procedure integrity and security control protection.

6.5.2 Computer Security Rating

The eCA uses safety strength and computer operation system

equivalent to Common Criteria EAL 4.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

eCA system development follows the CMMI and ISO 9001 to control the quality.

eCA hardware and software have to be specialized and only use components with security authorization. eCA will not install any hardware network connection and software components which are unrelated to eCA operations. Whenever being initiated, eCA will check if there is any malicious code.

6.6.2 Security Management Controls

When any eCA software being installed for the first time, it will be ensured this software provider provides the correct software and the software version is not revised. After the system installation, eCA will check the software integrity when it is initiated. On the other hand, software integrity will be performed routinely every month.

eCA will record and control every system configuration, modification and functional update; at the same time, eCA will detect any unauthorized modification of system software and configuration.

6.6.3 Life Cycle Security Ratings

Every year, there will at least one time evaluation on whether the length of the key has the risk of being compromised.

6.7 Network Security Controls

Neither eCA server nor interior repository connects to exterior network. Exterior repository connects to Internet to provide the uninterrupted certificates and ARL requesting services (unless necessary maintenance and backups).

Information stored in the eCA interior repository (including certificates and CARLs) is protected by the digital signature engine; it is transmitted manually from interior repository to exterior repository.

eCA exterior repository can prevent denial of services and intrusion attacks through the updates for system patch files, system vulnerability scanning, intrusion detection system, firewall systems and Filtering Router.

6.8 Engineering Controls

Follow the stipulations from section 6.1 and 6.2.

7 Certificate and CARL Profiles

7.1 Certificate Profile

The certificate profile field of the certificate issued by eCA shall comply with ePKI technical profile.

7.1.1 Version Numbers

The eCA shall issue X.509 v3 certificates.

7.1.2 Certificate Extensions

The certificate extensions field of the certificate issued by eCA shall comply with ePKI technical profile.

7.1.3 Algorithm Object Identifiers

The certificate issued by eCA shall use the following algorithm OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

(OID：1.2.840.113549.1.1.5)

The certificate issued by eCA shall use the following algorithm OIDs for identifying the algorithm for which the subject key was generated:

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 Name Forms

The subject and issuer fields of the certificate shall be complied with X.500 Distinguished Name and its attribute type

shall be complied with RFC3280.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The certificate policy object identifier field of the certificate shall use the OID of ePKI CP.

7.1.7 Usage of Policy Constraints Extension

The cross-certificate issued by eCA shall use this field if it is necessary.

7.1.8 Policy Qualifiers Syntax and Semantics

The certificate issued by eCA shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The eCA shall not set the critical certificate policy extension field.

7.2 CARL Profile

7.2.1 Version Numbers

The eCA shall issue X.509 v2 CARLs.

7.2.2 CARL Entry Extensions

The CARL issued by eCA shall comply with ePKI technical profile.

8 Maintenance

8.1 Change Procedure

The need for changes to this CPS should be periodically evaluated every year to sustain its assurance. The changes can be made in an annex to the CPS or by materially rewriting the CPS. If eCA CP or its OID has been changed, this CPS should be changed in accordance with the changed eCA CP or its changed OID.

8.1.1 Items that can Change without Notification

Only editorial change and typographical correction may be made to this CPS without notification.

8.1.2 Changes with Notification

8.1.2.1 Change Items

(1) Changes to items which will significantly impact the CAs, which are directly cross-certified with eCA, and relying party using this CPS should be posted in the repository of eCA for 30 days before the changes are made to this CPS materially.

(2) Otherwise, they should be posted for 15 days.

8.1.2.2 Notification Mechanism

Changes to all items in this CPS should be posted in the repository of eCA. If the items are subject to 8.1.2.1(a), a formal documented notification to the CAs that is directly cross-certified with eCA is required.

8.1.2.3 Comment Period

(1) If the items are subject to 8.1.2.1(1), the comment

period will be 15 days once their changes have been posted.

(2) If the items are subject to 8.1.2.1(2), the comment period will be 7 days once their changes have been posted.

8.1.2.4 Mechanism to Handle Comments

Any comments on the proposed changes should be received in the form posted in the repository of eCA before the deadline of comment period. All received comments will be reviewed and evaluated to decide the precise form and effective date of the changes.

8.1.2.5 Period for Final Change Notice

The changes to this CPS and their notification should be made in accordance with 8.1.2.2 and 8.1.2.3. According to 8.1.2.1, the changes should be posted at least for 15 days until the changed CPS goes into effect.

8.2 Publication and Notification Procedure

The revised CPS should be posted in the repository of eCA within 7 days, and it will be in effect once it’s posted, unless other specifications by PMA.

8.3 CPS Approval Procedures

After this CPS is approved by the authority concerned of MOEA, it should be posted by eCA. If the CP has been revised and posted, this CPS should be revised in accordance with the revised CP, and submitted to the authority concerned of MOEA for approval.

Unless there is other stipulation, if the revised content of this CPS contradicts to the original one, it will be a standard. If the changes of the CPS is achieved by appending document and the content of such document contradicts to the previous CPS, then this appended document will be a standard.