Unofficial Translation

Volume 126 Special Part 180 Ngor Government Gazette 16 December 2009

Notification of the Electronic Transactions Commission

Subject: Guidelines for the Preparation of the Certificate Policy and
the Certification Practice Statement
of the Certification Authority
B.E. 2552

To ensure that the services of the Certification Authority are reliable and have internationally acclaimed standards, the Electronic Transaction Commission deems it necessary to establish guidelines for the preparation of the certificate policy and the certification practice statement of the Certification Authority.

By virtue of Section 28 (6), Section 29 (7) and Section 37 (4) of the Electronic Transactions Act B.E. 2544 (A.D. 2001), the Electronic Transaction Commission hereby issues the following notification:

Clause 1 The Certification Authority shall prepare the certificate policy and the certification practice statement in accordance with the guidelines for the preparation of the certificate policy and the certification practice statement of the Certification Authority, as attached.

Clause 2 This notification shall come into force on the day following its publication in the Government Gazette.

Notified on the 8th day of October B.E. 2552
Sub Lieutenant Ranongrak Suwanchawee
Minister of Information and Communication Technology
Chairman of Electronic Transactions Commission

This translation is provided by Electronic Transactions Development Agency as the competent authority for information purposes only. Whilst Electronic Transactions Development Agency has made efforts to ensure the accuracy and correctness of the translation, the original Thai text as formally adopted and published shall in all events remain the sole authoritative text having the force of law.

Volume 126 Special Part 180 Ngor Government Gazette 16 December 2009

Guidelines for the Preparation of the Certificate Policy and the Certification Practice Statement of the Certification Authority

1. Introduction

Regarding the Subscriber's use of the electronic certificate issued by the Certification Authority to certify the holder of the certificate for use in the creation of a digital signature, which is one of the reliable categories of electronic signatures, or to certify the existence of a juristic person, or a server or any other Entity by application of the Public Key infrastructure or PKI technology, the reliability of the Certification Authority is regarded as critical to the service use and has a legally binding effect in various transactions made by the application of the electronic certificate to authenticate or certify the person, juristic person, server, or any other Entity for each transaction's performance.

To ensure the Certification Authority's service reliability, an agency called the Internet Engineering Task Force ("IETF"), which develops and promotes internet architecture, has set a framework or guideline for the establishment of the certificate policy and the certification practice statement of the Certification Authority. Such guideline is called the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647), which is an internationally recognised standard. It can be used as the guideline in the preparation of this notification for use in performing the preparation of the certificate policy and the certification practice statement of the Certification Authority in Thailand to conform to international standards.

2. Definitions and Acronyms

The definitions and acronyms displayed in this part shall provide correct meanings and understanding to the terms used in this document.

Terms/acronyms	Definitions
RFC	"The Internet Request For Comments" is a series of documents written to define or describe, at this moment in time, and recommend the certification practice statement with regard to protocol and internet policy etc.
Person	A natural person or a juristic person.
Entity	A person, including the server or the website or the operating unit / site, or any other device under a person's control.
Certificate Revocation List (CRL)	The electronic certificate revocation list is a list of revoked electronic certificates.
Online Certificate Status Protocol (OCSP)	The protocol for auditing the certificate revocation status and the start and end date and time for the use of such certificate.
Object Identifier (OID)	Value pairs which indicate any Information Object and such pairs are indicative of a peculiar code of such Object.
Public Key	The Public Key, which is used in the digital signature verification and can be used in the data message encryption to make such encrypted data message unintelligible, for the purpose of such data message's confidentiality.
Private Key	The Private Key, which is used in the digital signature creation and can be used in decryption where there is data message encryption to make such encrypted data message intelligible.
Key Pair	The Private Key and the Public Key in the asymmetric

	cryptosystem which is generated by making the Private Key mathematically related to the Public Key, thus to enable use of the Public Key in verification of whether the digital signature was created using the Private Key. Also, the Public Key can be used in the data message encryption to make the data message unintelligible for the data message's confidentiality, except for the person holding the Private Key. The holder of the Private Key can use such Private Key to decrypt the data message and enable the owner of the Private Key to read or understand the meaning of such data message.
Registration Authority (RA)	A person who is responsible for registration upon subscription application filing, notification of the revocation of the electronic certificate or renewal of the electronic certificate, and who shall audit and verify the accuracy of data provided by the Subscriber.
Compromise	This is when the data is lost, destroyed, amended, unduly disclosed or known of in a manner inconsistent with the repository objective of such data, including cases where there is a reasonable cause to suspect such circumstances.

3. Required Topics in the Certificate Policy and the Certification Practice Statement

Chapter 1	Introduction
Chapter 2	Publication and Repository Responsibilities
Chapter 3	Identification and Authentication
Chapter 4	Certificate Life-Cycle Operation Requirements
Chapter 5	Facility, Management and Operational Controls
Chapter 6	Technical Security Controls
Chapter 7	Certificate, CRL and OCSP Profiles
Chapter 8	Compliance Audit and Other Assessment
Chapter 9	Other Business and Legal Matters

4. Required Contents for the Certificate Policy and the Certification Practice Statement

Chapter 1 Introduction

This chapter's contents shall refer to categories of related persons or entities, and how to apply the certificate policy or the certification practice statement in practice.

1. Overview

This clause's material contents refer to the certificate policy and the certification practice statement in general, and applies the prepared certificate policy and the certification practice statement into practice upon PKI application, e.g. if there is a reliability level rating for different electronic certificates, such different certificates may have different complexities or different PKI usage scope. Therefore, the display of the PKI structure data is useful to understanding this part's content.

2. Document Name and Identification

This part's contents shall specify the "naming" the certificate policy and the certification practice statement or other identifier, including specifying the document's naming or such identifier's naming in technical terms. There is also the OID number registration requirement, with the official name of "ASN.1 Object Identifier". In practice, the OID number's designation in the certificate policy and the certification practice statement, or other identifier, is to enable an audit as to whether the certificate policy and the certification practice statement, or other identifier, that have been labelled with the OID number actually exist. This is because the OID number is related or connected to any Information Object; thus the identity of the OID number shall be in numerical order and separated by dots. There are several agencies which register the OID number, such as the American National Standard Institute (ANSI), USA, ISO etc.

3. PKI Participants

This chapter's contents should specify the identity and the category of the person or entity involved, including the roles and responsibilities of such person or entity.

3.1 Certification Authority

This is the Certification Authority which generates and issues the electronic certificate to certify the Public Key to the Subscriber.

3.2 Registration Authority

This is a person or an entity which has the duty to audit the subscription applicant, both in the subscription applicant’s identification stage on whether the subscription applicant is a person or an entity, and in the subscription applicant’s authentication stage on whether the subscription applicant is actually the person or the entity as the subscription applicant claims to be. In addition, the Certification Authority or the Registration Authority shall act uniformly in the revocation or renewal of the electronic certificate by auditing and verifying the accuracy of the data provided by the subscription applicant in several stages. After completion of the audit of the validity of the subscription applicant’s data, the Service Provider shall be notified to issue the electronic certificate to the subscription applicant. The Registration Authority may either be personnel of the Certification Authority or personnel of the subscription applicant, or another agency or entity entered into an agreement with the Registration Authority to perform such duty.

3.3 Subscriber

This is any person or entity to which the electronic certificate is granted by the Certification Authority.

3.4 Relying Party

This is any other person or entity that is reliant on the digital signature, which is one of the electronic signatures categories, or on the electronic certificate. Therefore, the Relying Party may or may not be a Subscriber of the Certification Authority. However, the Relying Party shall be the person who commits or refrains from any action due to its reliance on the electronic certificate or the digital signature. The Public Key contained in such electronic certificate shall be used in verifying the true identity of the subscription applicant who is the owner of the digital signature and whose name appears in the electronic certificate.

3.5 Other Participants

These are other persons or entities other than mentioned above, such as providers of repository services or outsourced Service Providers as the Certification Authority, etc.

3.6 Certificate Usage

This part's contents should set forth the identity or category of the electronic certificate which was applied into practice, such as: the electronic certificate to certify the person; the electronic certificate to certify the juristic person; the electronic certificate to certify the website; the electronic certificate to certify the server; the electronic certificate for use with the electronic mail or e-mail; and the electronic certificate for use with contracts or agreements etc.

Any certificate usage limitation or reliability level rating of the electronic certificate should be clearly specified. Also, if the certificate usage identity or electronic certificate type is so different as to necessitate the creation of the certificate policy or the certification practice statement for each usage identity or electronic certificate type, it is therefore necessary that such subject matter data be clearly specified.

3.7 Policy Administration

This part's contents should mention the name and address of the agency which drafts, registers, supervises and revises documents relating to the certificate policy and the certification practice statement, including the names and addresses of the contact people and their electronic mails, telephone numbers and fax numbers. Moreover, a position could be specified for being responsible for answering questions or communicating with the Subscriber of the Certification Authority.

In addition, to establish the reliability of the Certification Authority's services, in case the Certification Authority has prepared the certificate policy and the certification practice statement pursuant to the guideline notified by the Electronic Transaction Commission, there should be a mention of the Electronic Transaction Commission and the address of the Commission's administration unit in this clause.

3.8 Definitions and Acronyms

It is necessary that the preparation of the certificate policy and the certification practice statement refers to a substantial number of vocabularies and acronyms.

Therefore, such words or acronym meanings shall be given in this chapter - e.g. the meanings of the terms “the Certification Authority”, “the Registration Authority” , “the Subscriber”, “the certificate policy and the certification practice statement”, “the digital signature”, “the electronic certificate”, “the Key Pair”, “the Private Key”, “the Public Key”, “the entity”, etc. – so as to provide data accordingly to the Subscriber.

Chapter 2 Publication and Repository Responsibilities

This part’s contents shall specify the person who has repository duties for rendering the Certification Authority’s services, as well as whether such issuance of the electronic certificate was performed by the Certification Authority or derived from using another Service Provider’s service. Also, it shall specify the responsibilities of the person or agency with the duties of disseminating data regarding the certificate policy and the certification practice statement, as well as the contents that will be published, such as the security controls and the trade secret protection for important, sensitive data.

Moreover, relevant data on the data’s dissemination frequency or regularity, the access control of disseminated data, the certificate policy and the certification practice statement, or the status of the electronic certificate, including certificate revocation, should be provided.

Chapter 3 Identification and Authentication (I&A)

This chapter’s contents should provide data with regard to the steps used to authenticate a person or entity of the subscription applicant with the Certification Authority or Registration Authority prior to issuance of the electronic certificate, including prescribing the steps of authentication for a person of the Certification Authority, or Registration Authority or entity associated with rendering or jointly rendering services with the Certification Authority. In addition, this chapter may provide data regarding new electronic certificate issuance, electronic certificate renewal or certificate revocation. Nevertheless, the contents that shall be defined in this chapter, other than those mentioned above, are as follows:

1. Naming

The naming convention to identify the Subscriber should be defined as follows:

1.1 A naming convention such as X.500 Distinguished Name or RFC 822 Names shall be used for e-mails, and X.400 shall be used for names.

1.2 Such names may or may not have a meaning.

1.3 The name of the Subscriber in case of using anonymous or pseudonymous names or name concealment.

1.4 Rules on name conversion in various forms, such as X.500 and RFC 822 standard etc.

1.5 Such names must be unique names.

2. Initial Identity Validation

This part's data should prescribe identification and authentication procedures upon initial registration with the Certification Authority, the Registration Authority, the Subscriber or any other Relying Party, by:

2.1 Authentication of the relationship between the Private Key and the Public Key held by or in the possession of the Subscriber, such as the digital signature authentication which appears in the electronic certificate by means of using the digital signature in sending the certificate request message to the Certification Authority etc.

2.2 Authentication of conditions for verifying the existence of organisations or agencies, such as the verification from the affidavit of the company or the juristic person issued by the Department of Business Development, Ministry of Commerce etc.

2.3 Authentication of conditions for the data verification of the person acting on behalf of organisations or agencies, such as the verification from the power of attorney etc.

3. Identification and Authentication for Re-Key Requests

This step shall cover not only the step where the electronic certificate has expired, but also the electronic certificate usage revocation. Therefore, there should be a step with the same functional format as the identification and authentication of a person, which is the same as the initial subscription application step.

4. Identification and Authentication for Revocation Requests

This is to specify the class of person who can request certificate revocation, and the step for the authentication data of such person's identity, including such person's rights.

Chapter 4 Certificate Life-Cycle Operation Requirements

This part's data is used to specify the requirements used for operating the electronic certificate for the Certification Authority, the Registration Authority, the Subscriber and PKI participants to correspond with their roles and responsibilities.

1. Certificate Application

This part should specify the requirements for application for the electronic certificate, as follows:

1.1 The person who can apply for the electronic certificate, such as the certificate subject, or RA etc.

1.2 For the electronic certificate application procedure and related obligations, the electronic certificate application procedure's example may be as follows:

(1) A person files a certificate application and generates the Key Pair and files the electronic certificate application to the Registration Authority, whereby such person filing the certificate application must provide complete and accurate data in accordance with the electronic certificate application rules of the certification authority.

(2) The Registration Authority examines the application and countersigns the application that has undergone the Certification Authority's verification. The Registration Authority and Certification Authority must determine the

principles and procedures for the electronic certificate application.

2. Certificate Application Processing

This part's contents should provide data on the certificate application processing; examples thereof are as follows:

2.1 The Certification Authority and Registration Authority will audit the validity of the applicant for authentication.

2.2 The Certification Authority and Registration Authority will consider whether to approve or disapprove the subscription application of the electronic certificate.

2.3 The fixed term utilised by the Certification Authority and the Registration Authority in consideration of the application for the electronic certificate.

3. Certificate Issuance

This part's contents should provide data on the procedure of certificate issuance in the following matters:

3.1 Practice of the Certification Authority in certificate issuance, such as examination of the signature, and the Registration Authority's power and electronic certificate generation.

3.2 Notification of the certificate issuance results procedure to the Subscriber, e.g. notification by electronic mail.

4. Certificate Acceptance

4.1 Practice of the electronic certificate applicant which is accepted in the electronic certificate, i.e. the electronic certificate applicant accepts the electronic certificate issued by the Certification Authority in the following cases:

(1) The Certification Authority has not been informed in any way by the electronic certificate applicant within the prescribed period.

(2) The Subscriber has countersigned information notifying acceptance or non-acceptance of the electronic certificate.

4.2 Dissemination of the electronic certificate accepted by the electronic certificate applicant, which can be published via the X.500 Directory or LDAP repository.

4.3 Notifying other relevant persons with regard to the electronic certificate issued to the electronic certificate applicant, i.e. the Certification Authority may send the electronic certificate issued to the electronic certificate applicant to the Registration Authority.

5. Key Pair and Certificate Usage

5.1 Responsibilities of the Subscriber in the Key Pair and certificate usage, i.e. the Subscriber shall use the Private Key and electronic certificate in accordance with the policy defined in the certificate policy and contract between the Certification Authority and the Subscriber. The Subscriber can use the Private Key after the Subscriber has accepted the electronic certificate, and cannot use the Private Key and electronic certificate after the electronic certificate has expired or has been revoked.

5.2 Responsibilities of the Relying Party in the Subscriber’s Key Pair and certificate usage, i.e. the Relying Party shall use the electronic certificate pursuant to the policy defined in the certificate policy, and audit the status of the electronic certificate by using methods specified in the certificate policy, which is subject to the relevant Relying Party’s conditions.

6. Certificate Renewal

The certificate renewal means issuance of a new electronic certificate to the Subscriber without changing the Subscriber’s Public Key or any other data contained in the electronic certificate. The certificate renewal should consider the following matters:

6.1 Cases regarding certificate renewal authorisation, i.e. the electronic certificate has expired, but the policy permits continual use of the original Key Pair, thus enabling electronic certificate renewal.

6.2 Persons who are entitled to renew the electronic certificate, i.e. the Certification Authority, may allow the Registration Authority to apply for renewal on behalf of the Subscriber, or the Certification Authority may automatically renew the Subscriber's electronic certificate upon such electronic certificate's expiration.

6.3 There should be a clear procedure for electronic certificate renewal, such as password usage in the subject authentication prior to the electronic certificate renewal.

6.4 There should be a procedure to report to the Subscriber that the certificate renewal has been made.

6.5 There should be a specification of the procedure to accept the renewed electronic certificate by the Certification Authority for the electronic certificate Subscriber.

6.6 There should be an explanation of the electronic certificate dissemination and a procedure to inform PKI Participants of the certificate renewal.

7. Certificate Re-key

This part's contents should provide the data on the generation of the re-key, including new electronic certificate issuance to support the re-key by the Subscriber or any other party.

7.1 Cases regarding the Certification Authority's ability or requirement to generate the Key Pair and issue the electronic certificate to support the re-key, such as the certificate revocation or the Key Pair usage expiration.

7.2 Requirement that any person can apply for the electronic certificate to support the re-key.

7.3 There should be a procedure to inform the Subscriber of the issuance of the new electronic certificate.

7.4 There should be a specification of the procedure to accept the electronic certificate issued by the Certification Authority to support the re-key.

7.5 There should be an explanation of the electronic certificate dissemination and a procedure to inform PKI Participants of the certificate issuance to support the re- key.

8. Certificate Modification

This part's contents should provide data regarding new electronic certificate issuance due to data modification in the electronic certificate, other than the Subscriber's Public Key.

8.1 Cases regarding the Certification Authority's permission for the Subscriber to modify the electronic certificate data, such as a name change, change of its distinguished name and change of its role and obligation in the workplace.

8.2 Requirement that any person can apply for modification of the electronic certificate, e.g. the Subscriber, personnel authority or Registration Authority etc.

8.3 There should be a procedure to inform the Subscriber of the new electronic certificate.

8.4 There should be a specification of the procedure to accept the electronic certificate issued by the Service Provider.

8.5 There should be an explanation of the electronic certificate dissemination and a procedure to inform PKI Participants of new electronic certificate issuance.

9. Certificate Revocation and Suspension

This part's contents should provide data regarding certificate revocation and suspension.

9.1 Cases where the Certification Authority has effected suspension or certificate revocation, such as the Subscriber's employment termination, cryptographic equipment loss or existence of reasonable grounds to suspect that there is forbidden knowledge of the Private Key.

9.2 Requirement that any person, i.e. the Subscriber and the Registration Authority, is entitled to request the Subscriber's electronic certificate revocation and suspension.

9.3 There should be a specification of the procedure for electronic certificate revocation and suspension, such as the requirement that the Registration Authority or the Subscriber must countersign the electronic certificate revocation request.

9.4 There should be a specification of the time period when the Subscriber is entitled to request the electronic certificate revocation.

9.5 There should be a procedure to enable the Relying Party to verify the electronic certificate status.

9.6 Regarding the Certificate Revocation List (CRL) used in the dissemination of the revoked and suspended electronic certificate, there should be specification of such data's dissemination frequency, and the time period between CRL generation and CRL dissemination to the public. Also, if the online certificate status services are provided, the public should be informed of the relevant usage procedure, conditions and requirements.

9.7 There should be a specification of the electronic certificate's suspension period.

10. Certificate Status Services

This part's data is regarding the certificate status services for the Relying Party, and should contain the following matters:

10.1 Characteristics of the certificate status services and the availability of the life cycle, including the support policy during inability to render such services.

10.2 Characteristics of other related services.

11. End of Subscription

This part's data is regarding the Subscriber's practice steps at the end of subscription, which may be caused by the electronic certificate expiration or the Certification Authority's subscription termination.

12. Key Escrow and Recovery

The Certification Authority should determine the policy on the escrow and recovery of the Private Key and the session key encapsulation.

Chapter 5 Facility, Management and Operational Controls

This chapter's contents will cover the Physical Security and controls in case there is a requirement by the Certification Authority for secure key generation, subject authentication, certificate issuance, certificate revocation, and auditing and archiving.

Therefore, there should be a specification of the PKI participants' Security Techniques to build confidence in the electronic certificate usage and prevent penetration or access to the system or knowledge of the Certification Authority's life cycle data, including prevention of data errors in the generation of the electronic certificate or the certificate revocation list in case the Certification Authority's Private Key has been known about without permission.

Moreover, the physical security controls cover the following subject matters:

1. Site location and Construction

This chapter's contents should set up a high security zone or a safe room and safe box usage, installation of CCTV and a physical penetration detection system.

2. Physical Access

Entry and exit between the office zone and the high security zone should be indicated. Also, there shall be physical access protection for movement from one zone to another zone, such as being subjected to authentication prior to granting access to the life cycle, which can be achieved by using magnetic cards and verification of fingerprints etc. Moreover, notice should be taken with regard to the management of electrical and air-conditioning systems, protection against water peril, and backup media archives in other premises which are protected from unauthorised access and fire and water peril.

3. Physical Security Controls

The Certification Authority should describe the physical security controls of the workplace procedure as follows:

3.1 The site location of the Certification Authority and division of zones to respond to the level of security requirement.

3.2 The zone access control which requires different levels of security.

3.3 Monitoring of the electric power, circulation of water, control of the climate, temperature and relative humidity, and fire prevention; to prevent service interruption due to these causes.

3.4 Media archiving which is used in security archiving of the Certification Authority data; and there shall be a requirement for data backup outside the workplace to prevent the damage or loss of data.

4. Procedural Controls

The Certification Authority should assign appropriate roles and responsibilities to personnel in the organisation and establish the policy regarding the personnel's work in each role, such as the procedure for subject identification and authentication, or procedure, for access to key data by persons in different roles. This shall be done by having a division of duties, which forbids a person from undertaking duties in multiple roles for data security reasons.

5. Compromise and Disaster Recovery

The Certification Authority should have a Compromise and disaster recovery policy for events which Compromise data security, and for system disaster events, such as data destruction caused by an accident or any other cause, in order to prevent service interruption.

6. CA or RA Termination

In case the Certification Authority or Registration Authority ceases its business, the PKI participants, including those responsible for the Certification Authority data and the Registration Authority data, shall be informed accordingly in order to minimise impact to the Subscriber.

Chapter 6 Technical Security Controls

This part's contents specify security measures for keys and for data which authorises usage of the keys, such as a PIN number and password, and other matters related to key management.

1. Key Pair Generation and Installation

Key Pair generation and installation contains the following issues that shall be considered and set as policy:

1.1 Who generates the Key Pair to the Subscriber and was it generated by software or hardware?

1.2 Is the Security Techniques for the Subscriber to receive its Private Key viable?

1.3 Is the Security Techniques for the Certification Authority to obtain the Subscriber's Public Key viable?

1.4 How can the Relying Party securely obtain the Certification Authority's Public Key?

1.5 What is the Key Pair's length? That is, the keys may have the length of 1024 bit RSA and 1024 bit DSA.

1.6 Who is the person setting the Public Keys' parameters and are there any checking of qualitative parameters during key generation?

1.7 What are the objectives that the Key Pair may be used for, or the objectives of why the usage should be limited? These objectives should be consistent with key usage under version 3 of the X.509 standard.

2. Private Key Protection and Cryptographic Module Engineering Control

This part's contents should prescribe a procedure for Private Key protection and cryptographic module usage by the Certification Authority, the Registration Authority, the Subscriber and the data archiving Service Providers. Such procedure shall consider the security and damage resulting from the Private Key storage, Private Key backup and Private Key archival. The following questions shall be considered:

2.1 If the cryptographic module is used (may be software, hardware and/or firmware), which standard should be used as a reference?

2.2 Whether Private Key access by more than one authorised person has to be controlled (m out of n format)?

2.3 Is there any Private Key escrow policy?

2.4 Is there any Private Key backup policy?

2.5 Is there any Private Key archival policy?

2.6 In which case has the Private Key been transferred into or out of the cryptographic module?

2.7 Private Key storage in the cryptographic module shall be carried out by which method? For example, archive in the plaintext format, encrypted text format, split key format etc.

2.8 Who is the person eligible to use the Private Key and by which method?

2.9 Who is the person entitled to cancel the Private Key usage and by which method?

2.10 Who is the person entitled to destroy the Private Key and by which method?

2.11 What are the details of the cryptographic module's capabilities (may cite the relevant standards, such as FIPS 140-1)?

3. Other Aspects of Key Pair Management

This part should specify the procedure to manage and administer the Key Pair of the Certification Authority, Registration Authority, and the Subscriber and data archiving Service Providers by considering the following questions:

3.1 Whether there should be Public Key archival? If yes, who will perform the duty of Public Key archival and control the security of the Public Key archival system, in terms of necessity for continuous protection of the software and hardware which relates to Public Key usage?

3.2 What is the usage period for the electronic certificate and Key Pair of the Subscriber?

4. Activation data

This part's contents should specify the procedure to protect the data necessary for usage in activation, which may mean the reference code and installation code, used in authentication of the Subscriber in the certificate activation step, which is the data granted directly to the Subscriber by the Certification Authority or Registration Authority.

5. Computer Security Controls

This part's contents should describe the computer security controls to ensure reliability of the Certification Authority, e.g. the access control, the Certification Authority system's audit, subject identification and authentication, security testing and penetration testing. Such security control system must be subject to evaluation under international standards, such as the Trusted System Evaluation Criteria (TCSEC).

6. Life Cycle Technical Controls

This part's contents should mention the control of system development and the control of security management. The control of system development includes the security of the environment in system development, personnel executing the system development, and system design etc.

Control of security management means use of tools and procedure to ensure the security of the operational systems and the networks.

7. Network Security Controls

This part's contents prescribe the network security controls of the Certification Authority by preventing unauthorised access to the system via mechanisms of security equipment in multiple parts and hierarchies, e.g. the router, firewall and the Penetration Detection System: IDS.

8. Time-stamping

If time-stamping is required, it should be listed in this part. Also, the time source and its reliability should be stated.

Chapter 7 Certificate, CRL and OCSP Profiles

1. Certificate Profile

This part's contents describe the following matters (with reference to IETF RFC 3280):

1.1 Version of the supporting electronic certificate.

1.2 Data in the certificate extensions and criticality of such data and cryptographic algorithm Object Identifiers.

1.3 The name format of the Certification Authority, Registration Authority and Subscriber.

1.4 OID of the policy concerned.

2. Certification Revocation List Profile

2.1 This part's contents describe the following matters (with reference to IETF RFC 3280), the version of the supporting certificate revocation list:

2.2 The certificate revocation list and data in CRL Entry Extensions and the criticality of such data.

3. OCSP Profile

This part demonstrates the contents and format of the data used in the auditing of the certificate status using the OCSP protocol (Online Certificate Status Protocol), as well as other data, such as the version of the OCSP, and additional data that can be specified in the OCSP (with reference to IETF RFC 2560).

Chapter 8 Compliance Audit and Other Assessment

This part's contents shall prescribe items requiring the risk assessment or methodology used in the risk assessment, e.g. the risk assessment in accordance with the guideline of the WebTrust.

In addition, the frequency of the auditing or assessment of risk may be designated. The assessment shall be performed pursuant to the certificate policy and the certification practice statement and prior to the rendering of services, during the rendering of services, and for audit in case of the possibility of forbidden knowledge affecting the security.

There shall be specification of the required qualifications of personnel performing the audit and risk assessment duty and actions relating to such assessment results, such as the temporary suspension of operation or certificate revocation.

Chapter 9 Other Business and Legal Matters

This part's contents prescribe the collection of fees and financial responsibility, either in respect of the operation or a claim for damages arising from the service rendered, as well as various legal issues.

However, in preparation of the certificate policy and the certification practice statement, if the Certification Authority would like such document to be regarded as a contract or part of a service agreement, it may be necessary to consider additional content with regard to the limitation of liability in the certificate policy or the certification practice statement. If there is an intention to make the certificate policy and the certification practice statement as a contract or a part of the service agreement, it may be necessary to create a Subscriber agreement for the Relying Party which contains information regarding the limitation of liability of such person in rendering services.

1. Fees

Concerning the subscription fees, the Certification Authority rendering the service of certificate issuance, repository Service Providers or Service Providers acting as the Registration Authority may be authorised to collect certificate issuance or renewal fees, certificate access fees, fees for access to data regarding the revocation or latest status of the electronic certificate, fees for other services such as access to the certificate policy or the certification practice statement. Also, the Certification Authority may provide the refund policy.

2. Financial Responsibility

This part's contents should prescribe the operational PKI responsibilities and the responsibility to maintain the state of the Service Providers to remain solvent and pay damages. There may be additional contents concerning the financial amount of insurance coverage for liabilities and contingencies, assets on the balance sheet, surety bonds, letters of credit, indemnity, and may provide extended coverage by insurance or warranty.

3. Confidentiality of Business Information

As certain information is confidential business information, it is necessary to that there is confidentiality of such information, e.g. the business plan, sales information, trade secrets and information obtained from a third party under the non-disclosure agreement. Therefore, it is necessary to determine the extent of confidentiality for the information which is outside the confidentiality agreement's scope and liabilities of the PKI participants who have received such confidential information. There shall be a mechanism to promote confidence that there will be no events of Compromise.

4. Privacy of Personal Information

Regarding the services rendered by the Certification Authority, the Registration Authority or any other party providing relevant services, it is necessary that emphasis be given to privacy or confidentiality of the Subscriber's personal information. Only some disclosure of information can be made, such as information that must be disseminated by recording such in the electronic certificate, e.g. the Subscriber's name and family name.

Therefore, any operation involving personal information must be performed according to the laws governing such matters. If no such applicable law is in force, it may be necessary to perform such in accordance with the relevant matter's protection guidelines pursuant to international standards, e.g. the OECD Guidelines.

For this reason, any acts involving personal information should have the Subscriber's prior consent for such personal information disclosure. However, it is required that there are exceptions or necessary cases in which personal information can be disclosed, e.g. pursuant to various laws or a court order or an administrative order.

5. Intellectual Property Rights

There shall be specification of intellectual property rights, including the copyright, patent, trademark or trade secret for which the PKI participants may have, or exercise a claim for, as provided in the certificate policy and the certification practice statement, the electronic certificate, names, keys, or under the licence, or as set forth in any agreement with the PKI participants.

6. Representations and Warranties

This part requires the PKI participants to provide a warranty on the subject matters specified in the certificate policy or the certification practice statement, i.e.

the Certification Authority has to warrant that the data or facts recorded in the electronic certificate are accurate and correspond with the certification practice statement as prescribed in the service agreement, including cases which have to provide a warranty in other contracts or agreements, such as the Subscriber agreement and the Relying Party agreement.

7. Disclaimers of Warranties

The contents of the certificate policy or the certification practice statement shall define the disclaimers of warranties or prescribe the content regarding such matter in various service agreements.

8. Limitations of Liability

The limitations of liability may be stipulated for services provision, which may be determined by the nature of liability and the amount of damages subject to limitations of liability, such as the incidental damages, consequential damages etc.

9. Indemnities

Either party may be required to be liable for indemnities payment. There may be a specification in the certificate policy, certification practice statement or any other contract or agreement, i.e. the requirement that the Subscriber shall be liable for indemnities payment in case the Subscriber states data or facts required to be recorded in the electronic certificate which is false or untruthful; or the case where the Relying Party is liable for indemnities payment to the Certification Authority because of the failure to audit the revocation of the electronic certificate.

Regarding chapter 9, in addition to the above topics, the Certification Authority may additionally prescribe contents regarding contract termination and communication between the Service Providers and Subscribers, amendment of the certificate policy or the certification practice statement, dispute settlement, applicable laws and other contents.

References

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)