Ministry of the Interior
Certification Authority
Certification Practice Statement
Edition 1.2

Ministry of the Interior

2003.11.26

Directory

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 Ministry of the Interior Certification Practice Statements (hereinafter abbreviated as This Statement) are explained as follows:

(1) Competent authority approval no.: Chin-Shang-Tzu No. 09200201860

(2) Signed certificate:

(1) Category: natural person key certification

(2) Protection level: based on the level three operation of the assurance level of the government institution public key infrastructure certification policy (hereinafter abbreviated as Certification Policy), the Ministry of Interior Certification Authority will issue the signed and encrypted certificate with assurance level three defined by the certification policy.

(3) Applicable area: applicable to identity certification and information encryption required in e-government related applicable service in the open network. Subscribers and relying parties should carefully utilize the certificate signed by this authority and shall not violate the certification applicable area constrained and prohibited by this statement.

3. Major legal responsibilities:

(1) For the consequence caused on the subscriber or relying party by not abiding by the applicable area of the certificate utilization provided in this statement, this authority will not bear any legal responsibility.

(2) During occurrence of damage indemnity incident due to utilization of the certificate by the subscriber or relying party, the damage indemnity liability of this authority shall base on the responsibility area provided by related law.

(3) For damage incident caused by force majeure or other cause that cannot be blamed on this authority, this authority shall not bear any legal responsibility.

(4) For legal responsibility of the registration authority and the registration authority counter induced due to execution of business, unless otherwise provided by law, this authority shall be responsible.

(5) When the relying party encounters damage due to concealment of fact by the subscriber by providing incorrect information to the registration authority counter, if that damage cannot be blamed on the registration authority counter, the subscriber shall bear the responsibility of damage indemnity on its own.

(6) If the certificate of subscriber requires temporary suspension, recovery or revocation, it shall be processed based on related provision of this statement. If there is leakage of private key information or lost etc. that the certificate has to be revoked, the subscriber should immediately notify this authority. However, such subscriber shall still bear the legal responsibility due to utilization of that certificate before such alteration.

4. Other important matters:

(1) If part of the certification service has to be suspended temporary due to requirement of system maintenance, alteration and expansion of this authority, then it will be announced in the repository and subscribers will be notified.

Subscribers or relying parties cannot base on this to be the reason to request for damage indemnity from this authority.

(2) After the subscriber has accepted the certificate issued by this authority, that means the accuracy of the certificate content information is confirmed and the subscriber shall utilize the certificate based on related provision of this standard. If there is error in the certificate content information, the subscriber shall actively notify this authority.

(3) Subscribers and relying parties should carefully select safe computer environment and reliable application system. If there is damage on the rights and interests of the user due to the computer environment or the application system itself, the user shall bear the responsibility on its own.

(4) If this authority cannot operate normally due to reason, subscribers or relying parties should immediately seek for other route to complete the legal behavior with other party and cannot base on the reason that this authority cannot operate normally as the cause of rebuttal on other party.

(5) When the relying party accepts the certificate issued by this authority, that means the subscriber understands and agrees on the terms of the legal responsibility of this authority and shall utilize the certificate based on the related provision of this statement.

1. Preface

The Ministry of the Interior Certification Authority Certification Practice Statement (hereinafter abbreviated as this statement) is stipulated based on the Certificate Policy of the Government Public Key Infrastructure, hereinafter abbreviated as the Certificate Policy and by following the related provision of items that should be clearly stated in the Electronic Signature Law and Certification Practice statement. It explains how the Ministry of the Interior Certification Authority, MOICA, hereinafter abbreviated as this Certification Authority can abide by the provision of assurance level 3 of the certification policy to conduct issue and management of the natural person public key certificate.

1.1 Outline

According to the provision of the certification policy, this authority is the Level 1 Subordinate CA of the Government Public Key Infrastructure, CPKI, hereinafter abbreviated as Infrastructure). In this infrastructure, the authority is responsible for the issue and management of the natural person certificate including two certificates for signing and encryption and these are all level 3 certificate of the certificate policy assurance.

In this statement, it will explain the certification practice of this authority so as to ensure that the usage of the certificate and management can conform to the provision of policy assurance level 3 stipulated by the certification policy. The practice standard stated in this statement is only applicable to the related entity of this authority such as this authority, registration authority, registration authority counter, card management center, subscribers, relying parties and repository etc. The Ministry of the Interior is the competent authority of this authority that is responsible for the stipulation and revision of this statement. This statement can only be executed upon approval by the Ministry of Economic Affairs, the competent authority of the Electronic Signature Law. This standard is not authorized to be utilized by certification institution beyond this authority. For any problem caused due to utilization of this standard by other certification institution, such certification shall bear its own responsibility.

1.2 Identification of the certification practice statement

The name of this standard is called Ministry of the Interior Certification Authority Certification Practice Statement and this edition is 1.2. The announcement date is November 26 2003. The latest edition of this statement can be obtained from the following homepage:

http://moica.nat.gov.tw/.

This statement is stipulated based on the certification policy and the operation of this authority following the provision of the certification policy assurance level 2 and its article identification name is id-tw-gpki-certpolicy-class-3Assurance and the article identity code is {id-tw-gpki-certpolicy 3}. (Please refer to certification policy).

1.3 Main members and certification applicable area

Related members that participated in the certification service of this standard include:

(1) This authority
(2) Registration authority
(3) Registration authority counter
(4) Card management counter
(5) Repository
(6) End entities

1.3.1 Ministry of the Interior Certification Authority

This authority is the first level subordinate certification authority in this infrastructure and by abiding the provision of certification policy assurance level 3, this authority is responsible for the issue and management of certification of natural person.

1.3.2 Registration authority

This authority will establish the registration authority responsible for collecting and certifying the identity of the subscriber and the registration of related information of certification. The registration authority is formed by many registration authority counters (RA counter).

The registration authority server (RA server) is established in the registration authority responsible for certifying the identity of the certification authority officer (RA officer and hereinafter abbreviated as RAO) and the registration authority center. Management of the registration authority server is the responsibility of the RA officer who will set the RAO account number and authority limit on the registration authority and produce and issue the RAO IC card. The RA server is installed with private key and the communication between the RA server and this authority server shall be protected by the private key signature of the authority.

1.3.3 Registration authority counter

Registration authority counter can be established in the household administration offices in various jurisdictional cities, counties (cities) or it can be undertaken by organization authorized and approved by this authority. Apart from within that organization, its establishment location can be established in temporary mobile location depending on requirement.

The RAO of the registration authority counter is responsible for the operation or the RA counter in accepting the processing of registration application, temporary suspension application, utilization recovery application and revocation application etc.

1.3.4 Card control center

The token utilized by the subscribers of this authority is IC card. This authority will consign reliable card management center to conduct IC card production and management. IC card production and management operation includes internal key pairing inside the card and is based on random number to set the primary identification code of the IC card (hereinafter abbreviated as the PIN number) and the allocation management of IC cards.

1.3.5 Repository

The repository is responsible for announcing the certificate issued by this authority, certificate revocation list, CRL and other related certification information.

Apart from the self-establishment and maintenance and operation of the repository, this authority will transfer and store the certificate and

certificate revocation list issued by this authority in the directory service, DS of this authority.

The repository provides 24 hours all day service and the website is : http://moica.nat.gov.tw/.

1.3.6 End entities

1.3.6.1 Subscribers

Subscribes of this authority refers to the certificate subject name entities issued and recorded in this authority. For natural person certificate that its issue is the responsibility of this authority, subscriber means citizen of Republic of China over 18 years of age and has established domicile in the country.

1.3.5.2 Relying parties

Relying parties refers to the certificate subject name and the entity of the connecting relationship of the public key.

Before the relying party utilizes the certificate issued by this authority, it is necessary to base on the certificate and the certification status information of this authority itself to examine the validity of the certificate utilized. Only after confirming the validity of the certificate, then the certificate can be utilized to conduct the following operations:

(1) Examine the integrity of the electronic document.

(2) Examine the identity of the electronic document generator.

(3) Establish a safe communication channel between the certificate subject entities.

1.3.7 Applicable area

1.3.7.1 Applicable area of certificate

The certificate issued and managed by this authority is the natural person certificate who is over 18 years old Republic of China citizen and has established its domicile and that includes signature and encrypted certificate.

Certificate issued by this authority conforms to the provision of certificate policy assurance level 3 and is applicable in identity certification required by e-government in the network and information encryption.

1.3.7.2 Certificate utilization constraint

When using the private key, subscriber should carefully select a safe computer environment and reliable application system so as to avoid theft of the private key by malicious software and its misuse resulting in damage on the rights and interests.

Before utilizing the certificate issued by this authority, the relying party should confirm whether the category of the certificate, assurance level and key usage etc. could conform to the application requirement.

The relying party should base on the X.509 standard to process the critical and non-critical certificate extensions.

Before utilizing the certification service provided by this authority, the relying party should careful read this statement and abide by the provision of this statement. At the same time, such party should pay attention to the revisions on this statement.

1.3.7.3 Prohibition in the utilization of certificate

(1) Commit crime.

(2) Military order and battle situation and nuclear bio-chemical weapons control.

(3) Nuclear power operation equipment

(4) Aviation flying and control system.

1.3.8 Certification service in the form of outsourcing

This Ministry shall base on the Government Purchase Law to consign Chunghwa Telecommunication Co. Ltd. to process the establishment and maintenance and operation of this authority. The name list of the outsourcing targets shall be announced in the website.

Website: http://moica.nat.gov.tw

2.1 Contact method

1.4.1 Formulation of the certification practice statement and the competent authority

This authority is responsible for formulating various terms of this statement. The formulation and revision of this statement shall be published and executed after approval by Ministry of Economic Affairs that is the competent authority of the Electronic Signature Law.

1.4.2 Contact information

If there is any suggestion on this statement, please contact this authority. The contact phone of this authority : 02-25132253, mailing address: No. 4, Sung Chiang Road, Lane 469, Taipei 104, email: moica@moi.gov.tw. Please refer to http://moica.nat.gov.tw/.

1.4.3 Examination of the certification practice statement

According to the related provision of the Electronic Signature law, this statement is required to be approved by the Ministry of Economic Affairs, the competent authority of the Electronic Signature Law first before providing certificate issue service to outside.

3. General terms

2.1 Responsibilities and obligations

2.1.1 Responsibilities of the Ministry of the Interior Certification Authority

(1) Operate with this statement based on the provision of certification policy assurance level.

(2) Issue and announce the certificate, however subscriber can decide on its own whether its certificate can be announced.

(3) Revocation, suspension and recovery of certificate utilization.

(4) Issue and announcement of the revocation list.

(5) Execute the identification and authentication procedure of related personnel of this authority.

(6) Safe production of the private key of this authority.

(7) Protect the private key of this authority.

(8) Support the registration authority to conduct related operation in certificate registration.

2.1.2 Responsibilities of the registration authority

(1) Transmit the application information and open key of the subscriber to this authority through safety channel.

(2) Advise subscribers and relying parties on the obligations and responsibilities regarding this authority and the registration authority.

(3) Advise subscribers and relying parties that in regard to accepting or utilizing the certificate issued by this authority, it is necessary to abide by the related provision of this standard.

(4) Execute the identification and authentication procedure of RAO.

(5) Safe production of private key of the registration authority.

(6) Protect the private key of the registration authority.

2.1.3 Responsibilities of the registration authority counter

(1) Provides various counter application for certificates and executes identity identification and authentication procedure of counter application for certificate.

(2) Responsible for individualized card production service of IC card and provides certificate acceptance operation.

2.1.4 Responsibilities of the card management authority

(1) Based on the provision of 6.1.1.1, drive the IC card so as to match the key of the subscriber in the internal safe production.

(2) Set the initial PIN number of the IC card with the initial code.

(3) Provides IC card opening information management operation.

(4) Provides IC card locking management operation.

(5) Execute IC card distribution management operation

2.1.5 Obligation of subscribers

(1) It is necessary to abide by related provision of this statement and confirm the accuracy of the provided application information.

(2) After this authority has approved the certificate application and the certificate is issued, subscriber should accept the certificate based on the provision of section 4.3.

(3) After the subscriber has accepted the certificate issued by this authority, that means the subscriber has confirmed the accuracy of the information content of the certificate and will utilize the certificate based on the provision in section 1.3.7. If there is error in the information content of the certificate, the subscriber should actively notify this authority.

(4) Subscriber should properly keep and use the certificate IC card.

(5) If it is necessary to suspend the utilization temporary, restore its utilization, revoke or re-apply the certificate, subscriber should process based on the provision in section 4.4. If there is leakage or lost of private key information and it is necessary to revoke the certificate, subscriber should notify this authority. However, subscriber should still bear the legal responsibility of utilizing that certificate before the alteration.

(6) Subscriber should carefully select safe computer environment and reliable application system. Due to the factor of computer environment or the application system itself resulting damage to the rights and interests of the relying parties, the subscriber shall bear responsibility on its own.

(7) When normal operation cannot be conducted due to reason when utilizing the certificate, the subscriber should try to seek other route as soon as possible to complete the legal behavior that should be conducted with other party. The subscriber cannot base on the reason that the normal operation cannot be conducted as the reason to rebut other party.

2.1.6 Obligation of the relying parties

(1) When utilizing the certificate issued by this authority or during inquiry with the repository of this authority, it is necessary to abide by the related provision of this standard.

(2) When utilizing the certificate issued by this authority, it is necessary to check the assurance level of this certificate first so as to ensure the

rights and interests.

(3) When utilizing the certificate issued by this authority or the certificate revocation list, it is necessary to check the digital signature first so as to confirm whether such certificate or certificate revocation list is correct.

(4) When utilizing the certificate issued by this authority, it is necessary to confirm the usage of the key recorded in the certificate.

(5) When utilizing the certificate issued by this authority, it is necessary to check the certificate revocation list first in order to confirm whether such certificate is valid.

(6) It is necessary to carefully select a safe computer environment and reliable application system. Due to the factor of computer environment or the application system itself resulting damage to the rights and interests of the relying parties, the relying party shall bear responsibility on its own.

(7) When normal operation cannot be conducted due to reason when utilizing the certificate, the relying party should try to seek other route as soon as possible to complete the legal behavior that should be conducted with other party. The relying party cannot base on the reason that the normal operation cannot be conducted as the reason to rebut other party.

(8) When accepting the certificate issued by this authority, that means the relying party has understood and agreed on the related terms of legal responsibility of this authority and will utilize the certificate according to the scope provided in section 1.3.7.

2.1.7 Obligation of the repository service

(1) Certificates issued, certificate revocation list and other related information of certificates would be announced periodically based on the provision of section 2.6.

(2) Announce the latest information of this statement.

(3) The access of the repository shall be processed based on the provision of 2.6.3.

(4) Guarantee the receiving status and usability of the repository information.

2.2 Legal responsibility

2.2.1 Responsibility of the Ministry of the Interior Certification Authority

2.2.1.1 Guarantee area and its limitation condition

This authority shall operate based on the certification policy assurance level 3 and shall abide by this procedure of this statement to issue and

manage certificate, issue and announce the certificate revocation list and will maintain the normal operation of the repository.

2.2.1.2 Denial declaration and its limitation condition

If the subscriber or relying party cannot base on the applicable area provided in section 1.3.7 to utilize the certificate, for the consequence induced, this authority shall not bear any legal responsibility.

2.2.1.3 Other exception terms

If due to force majeure or other cause that cannot be blamed on this authority, for the damage case caused, this authority shall not bear any legal responsibility.

If part of the certification service has to suspended temporary due to system maintenance, alteration and expansion of this authority, then it shall be announced in the repository and subscribers will be notified. Subscribers or relying parties cannot base on this as the reason to request this authority for damage indemnity.

If it is due to the cause of certification revocation in section 4.4.1, subscriber should present certificate revocation application with this authority based on the certificate revocation procedure in section 4.4.3. Within one working day, this authority will approve the application for certificate revocation and complete the certificate revocation operation, issue the certificate revocation list and announce it in the repository. Before the certificate revocation status is not yet announced, subscriber should adopt appropriate action so as to reduce the effect on relying parties and shall bear all responsibilities caused by utilization of such certificate.

2.2.2 Responsibility of the registration authority

2.2.2.1 Guarantee area and its limitation condition

the registration authority shall abide by the procedure specified in the statement and is responsible for collecting and certifying the identity of subscribers and registration of related information of certification.

The registration authority is formed by multiple registration counters. For the legal responsibility caused by execution of registration work by the registration authority, except otherwise provided by law, this authority shall be responsible.

The certificate issued by this authority will only conduct confirmation on the certificate subject and the RAO will examine the identity of subscribers and related information of the certificate. If the subscribe conceals its facts and provides incorrect information to the registration

counter causing damage on the relying party. If that damage caused cannot be blamed on the registration counter, then the subscriber shall bear the damage indemnity liability.

2.2.2.2 Denial declaration and its limitation condition

Subscribers and relying parties shall utilize the certificate according to the applicable area provided in section 1.3.7.

2.2.2.4 Other exceptional terms

For damage caused by force majeure or other causes that cannot be blamed on the registration authority, the registration authority shall not bear any legal responsibility.

2.2.3 Responsibility of the card management center

The card management center shall abide by the procedure specified in the standard and is responsible for driving the IC card to product key pair of the subscriber and related card issue operation. The legal responsibility generated by the execution of card management operation by the card management center shall be the responsibility of this authority.

2.3 Financial responsibility

This operation of the authority shall be maintained by this Ministry that will compile budget and insurance is not conducted with insurance company. However, the audit authority shall conduct financial and accounting audit on our Ministry and the other financial responsibility shall be processed based on the provision of related laws and regulations.

2.4 Interpretation and execution

2.4.1 Applicable law

Due to the execution of certificate issue and management operation requirement, for the explanation and legality of related agreements signed by this authority, it shall be processed according to the provision of related laws and regulations.

2.4.2 Divisible, existence and continuance, merger and public announcement notice

If any one chapter or section of this standard is incorrect or invalid, the other chapters and sections will still remain valid. The revision on this statement shall be processed based on the provision of Chapter 8.

2.4.3 Dispute processing procedure

If there is dispute between the subscriber and this authority, both parties shall base on the principle of trust to conduct negotiation and discussion. If the negotiation fails and litigation is required, the Taiwan Taipei

District Court shall be the first trial jurisdictional court.

2.5 Fees

2.5.1 Certificate issue and exhibition fee

Please go to the website to inquire on related fees : http://moica.nat.gov.tw/.

2.5.2 Certificate inquiry fee

Please go to the website to inquire on related fees : http://moica.nat.gov.tw/.

2.5.3 Certificate revocation and status inquiry fee

Please go to the website to inquire on related fees : http://moica.nat.gov.tw/.

2.5.4 Other service fee

Please go to the website to inquire on related fees : http://moica.nat.gov.tw/.

2.5.5 Refund request provision

When the certification applying party applies for the certificate based on the provision of section 4.2.2 and if processing cannot be conducted based on provision, for the prepaid IC card handling fee, such party can present refund application at the counter. It is required to deduct handling fee from the refund (20% handling fee of the IC card). For related provision, please go to website to inquire : http://moica.nat.gov.tw/.

2.6 Announcement and repository

2.6.1 Information announcement by the Ministry of the Interior Certification Authority

(1) Certification policy
(2) This statement
(3) Certificate revocation list
(4) Certificate of this authority itself (till the duration of all certificates signed by the private key corresponding to the public key of that certificate).
(5) For the issued certificate, only the subscriber can decide on whether its certificate can be announced.
(6) Certificate temporary suspension information or other certificate related information.
(7) Privacy right protection policy.
(8) Latest audit result.
(9) Latest information of this authority.

2.6.2 Announcement frequency

(1) This statement shall be announced upon approval by the competent authority. Revision on this statement shall be announced based on the

provision of Chapter 8.

(2) This management center shall issue one certificate revocation list every day that will be announced in the repository.

(3) The certificate of this authority itself will be announced in the repository when it is issued.

(4) For the issued certificate, it will be announced in the repository when it is issued.

(5) The certification policy will be announced upon approval by the e-government competent authority. The subsequent revision shall be announced based on the provision of Chapter 8 in certification policy.

2.6.3 Access control

The mainframe of this authority is established inside the firewall and the outside cannot be connected on line with this mainframe directly. The depository mainframe shall be controlled and managed through the firewall system and will be directly connected to the database of the mainframe of this authority to retrieve certificate information or download certificate.

In regard to the information announced by this authority in section 2.6.1, it is mainly provided to subscribers or relying parties for inquiry. Therefore it is opened for reading and access and in addition, in order to protect the safety of the repository, access control will be conducted and its access status and usability shall be maintained.

2.6.4 Repository

This authority shall be responsible for the management of the repository. If normal operation cannot be conducted, within two working days, normal operation will be restored. The website of the repository is: http://moica.nat.gov.tw.

2.7 Audit method

2.7.1 Audit frequency

This authority shall accept external audit on this infrastructure once a year and irregular internal audit so as to confirm that the related operation can conform to the safety provision and procedure stipulated in this statement.

2.7.2 Audit personnel identity and qualification

The e-government competent authority shall base on the government purchase law to subcontract the processing of the external audit operation of the infrastructure certification organization. Audit company that is familiar with the related provision of this infrastructure and the operation of this authority will be consigned to provide fair and objective audit service. During the audit, this authority shall conduct identity identification on the audit personnel.

2.7.3 Relationship between the audit personnel and the party to be audited

By coping with e-government competent authority to conduct the external audit operation of this infrastructure certification organization, audit company will be consigned to conduct audit on the operation of this authority.

2.7.4 Auditing area

(1) Whether this authority operates based on this standard.
(2) Whether this standard conforms to the provision of the certification policy.
(3) Whether the registration authority and the registration authority counter operate based on this standard and related provision.
(4) Whether the card management center operates based on this standard and related provision.

2.7.5 Response method on the audit result

If audit personnel discovers that the establishment and operation of this authority does not conform to the certification policy and the provision of this standard etc., the following actions shall be adopted:

(1) Record the condition of inconformity.
(2) Notify this authority on the condition of inconformity.
(3) For items that do not conform to provision, this authority will improve immediately and will notify the audit personnel to conduct repeat audit.
(4) According to the type of inconformity, seriousness and the time required, this authority will adopt temporary suspension of operation, revoke issue of subscriber certificate or other coping activities.

2.7.6 Area of the publicized audit result

This authority 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 Information confidentiality area

2.8.1 Confidential information category

The following information generated, taken over or kept by this authority shall be deemed as confidential information.

(1) Private key and password utilized in the operation of this authority.

(2) Kept information of the separate holding of the key of this authority.

(3) Application information of the subscribe certificate that cannot opened or provided to third party for usage without consent by the subscriber or conforming to the provision of laws and regulations.

(4) Record generated or kept by this authority that can be provided for audit and follow up.

(5) Audit record and report generated in the audit course by the audit personnel cannot be publicized completely.

(6) Operation related documents that are listed as confidential level.

The present and resigned employee of this authority can strictly keep secret on the confidential information

2.8.2 Non-confidential information category

(1) The issue certificate, revoked certificate and the certificate revocation list announced by the repository of this authority shall not be deemed as confidential information.

(2) Except otherwise agreed, identification information or information recorded in the certificate shall not be deemed as confidential information.

2.8.3 Publication of information of certificate revocation or temporary suspension

Information of certificate revocation or temporary suspension will be announced in the repository of this authority.

2.8.4 Information release in response to judicial authority request

Due to requirement of investigation or evidence collection, if the judicial authority, supervision authority or public order authority requires inquiring on the confidential information in Section 2.8.1, it shall be processed based on legal procedure and there will be separate notification to the subscriber. However, this authority reserves the right to collect

reasonable fees from the authority applying for inquiry.

2.8.5 Information release in response to subscriber request

Subscriber can apply to inquire on its own certificate application information in section 2.8.1 (3). This authority will notify the subscriber by mail or email. However, this authority reserves the right o collect reasonable fees from the subscriber applying for inquiry.

2.8.6 Other information release condition

It will not be provided for commercial application and in regard to release of other information and it will be processed based on provision of related laws and regulations.

2.8.7 Privacy right protection

This authority will base on the computer processing of individual information protection law to process the application information of subscribers. The certificate content will record the Chinese name of the subscriber and the last four digits of the national identity card number. Therefore, the national identity card number of the individual will not be disclosed due to announcement of certificate. In addition, for the individual email address, the subscriber will decide whether it is to be recorded in the certificate. At the same time, the subscriber can self decide on whether its certificate can be announced in the repository of this authority so as to protect the privacy of the individual information of the applying party.

2.8.8 Intellectual property right

The key of this authority and the separate holding of key is the intellectual property of this authority. The token utilized by subscriber is the IC card. The card management center trusted by this authority will drive the IC card and the IC card will self produce the key pair and the intellectual property right of that key pairing will belong to that subscriber.

The certificate and certificate revocation list issued by this authority is the intellectual property of this authority.

This authority will try as much as possible to ensure the accuracy of the subscriber name but will not guarantee the intellectual property right belonging of the subscriber name. If there is dispute on the subscriber

name, the subscriber shall process based on legal procedure and submit that processing result to this authority so as to ensure the rights and interests.

For related documents written due to execution of the certification authority operation of this authority, its intellectual property right shall be owned by this Ministry.

The intellectual property right of this standard is owned by this Ministry. This standard can be freely downloaded from the repository of this authority or it can be reproduced or distributed based on related provision of the copyright law. It is necessary to guarantee it is completely duplicated and it should be indicated that the copyright is owned by this Ministry. In addition, party who reproduces or distributes this standard cannot collect fees from other party and cannot refuse the request of any party to acquire this standard. For all results due to improper utilization or distribution of this standard, this Ministry will not bear any legal responsibility.

3. Identification and examination procedure

3.1 Initial registration

3.1.1 Naming category

For the certificate subject name of the certificate issued by this authority, the X.500 distinguished name, DN will be adopted.

3.1.2 Requisite meaning in meaning

The name of the subscriber of this authority is mainly based on the Chinese name stored in the household administration system database of this Ministry.

3.1.3 Naming form explanation rules

According to the certificate format analysis of the infrastructure technical standard, the explanation rules of various naming form shall be defined based on the ITU-TX.520 name attribute.

3.1.4 Naming uniqueness

The X.500 distinguished name of this authority is:

C=TW, O=Executive Yuan, OU=Ministry of the Interior Certification

Authority

In order to allow the certificate subject name of the certificate issued by this authority to possess uniqueness, the format of the subscriber X.500 distinguished name adopted by this authority is:

G=TW, CN=the Chinese name stored in the household administration system database of this Ministry,

serialnumber=the only serial number given to that subscriber automatically by this authority

3.1.5 Naming dispute solution procedure

This authority permits similarity of the domicile Chinese name of the subscriber. However, it will be distinguished based on the serialNumber of the distinguished name so that the name of the subscriber can maintain its distinction.

However, when the automatic granted serial number is repeated, this authority will base on manual awarding method to maintain the distinction of the serialNumber in order to solve the problem of naming dispute.

3.1.6 Trademark identification, authentication and role

Not applicable

3.1.7 Method of certifying possession of private key

The card management center trusted by this authority will drive the IC card and will self produce key pair inside the card. During issue of certificate, the public key of the subscriber will be publicly transmitted to this authority from the registration authority counter via safety channel.

3.1.8 Organization identity authentication procedure

Not applicable. The certificate issue target is natural person and there is no identity authentication procedure.

3.1.9 Personal identity authentication procedure

After the certificate applicant himself/herself has shown the national citizen identity card original copy, the RAO at the registration authority counter should check with the household administration office whether such national citizen identity card is valid and whether

the person recorded in this national citizen identity card is actually that applicant so as to confirm the identity of such applicant.
At the same time, it is necessary to check whether the applicant is a national citizen who is over eighteen years old and is established with domicile.

3.1.10 Hardware installation or server software authentication procedure

The certificate target issued by this authority is natural person and there is no hardware installation or server software authentication procedure.

3.2 Certificate key replacement or extension

3.2.1 Certificate key replacement

Certificate key replacement means the issue of a new certificate that has similar characteristics and guarantee etc. as the old certificate.
For the new certificate, except that it has new and different public key (compared with the new one, different private key) and different serialNumber, it may be assigned with different validity time limit.
If the utilization period of private key of the subscriber is due and is required to replace the key, the subscriber should reapply for certificate with this authority. Based on the provision of section 3.1, the registration authority counter will conduct identification and authentication on the certificate reapplication subscriber.

3.2.2 Certificate extension

As the validity period issued by this authority is given with the longest validity period based on the stipulation in the certification policy, therefore extension on the issued certificate is not permitted in order to maintain the safety of the key.
When the key is due, it is necessary to base on the new key to reapply for certificate. Its required identity identification and authentication procedure is similar to the provision of section 3.1.

3.3 Certificate revocation key replacement

If the private key of the subscriber needs to be replaced due to certificate revocation, it is required to reapply for certificate with this authority. The registration authority counter will base on the provision of section 3.1 to conduct identification and authentication on the subscriber reapplying for

the certificate.

3.4 Certificate revocation

The authentication procedure of the certificate revocation application is similar to the provision of section 3.1.

3.5 Certificate content alteration

The authentication procedure of the certificate content alteration application is similar to the provision of section 3.1.

4. Operation standard

4.1 Certificate application procedure

Applicant should first read the subscriber agreement. If the subscriber agrees on the content of the terms, then the subscriber will conduct certificate application.

This subscriber agreement will be recorded in the website of this authority (http://moica.nat.gov.tw) and the certificate application.

4.1.1 First time certificate application

When applying for the certificate at the counter, the certificate applicant should provide its original copy of the national citizen identity card. Upon receipt of the certificate application, the authority registration counter will base on the provision of section 3.1.9 of this statement to conduct identity authentication procedure to serve as the basis for the authority to judge whether to agree on the issue of certificate.

During on-line application, the applicant should go to the on-line website to fill in the certificate application information. After filling in its email address and subscriber password etc., the subscriber shall still bring its original copy of the national citizen identity card so as to serve as a basis for the authority to judge whether to agree on the issue of certificate.

4.1.2 Certificate application during alteration of certificate content

When there is alteration on the identity information such as personal name or national citizen identity card number of the subscriber, then for the original certificate, it is necessary to apply for revocation first or this authority will revoke the certificate automatically. In addition, the altered name or national identity card number will be utilized to conduct reapplication for the certificate so as to complete the alteration of identity

information recorded in the certificate in regard to name or national citizen identity card number. When reapplying for certificate, it can base on the procedure provided in section 4.1.1 to process.

Depending on the requirement of the application, subscriber can alter the email address recorded in the certificate. Then it is necessary to apply for certificate revocation and then followed by utilizing the altered email address to conduct certificate reapplication. When reapplying for certificate, it can be processed based on the procedure provided in section 4.1.1.

4.1.3 Certificate application during lost of certificate

If the subscriber once owned the certified IC card, but it is lost or destroyed and cannot be used, then it is necessary to apply for new certified IC card. Before application, it is necessary to base on the provision of section 4.4.3 to revoke the lost or destroyed certificate and then apply for new certificate based on the provision of section 4.4.1.

4.1.4 Certificate application when the certificate is due

Two months before the certificate validity is due or after the validity period of the certificate is expired, if the subscriber requires utilizing the certificate, the subscriber can reapply for certificate based on the method in section 4.1.1.

4.2 Certificate issue procedure

4.2.1 Application for certificate at the counter

The issue of certificate can be completed based on the following steps:

(1) After confirming the identity of the certificate applicant, the RAO will input the information of the certificate application into the registration authority counter system

(2) Upon confirming that the input information is correct, the RAO will utilize its IC card to sign the digital signature on the certificate application information and will then conduct IC card personalized outer-appearance printing.

(3) The related certificate application information will be uploaded to the registration authority.

(4) Upon examination that there is no error on the signature of RAO, the registration authority will base on completed certificate application message to apply for certificate with the certificate authority.

(5) The certificate authority will resend the issued certificate and the issued certificate will be written in the IC card of the applicant through the registration authority counter system.

4.2.2 Application for certificate on-line

The issue of certificate shall be completed based on the following steps:

(1) Upon confirming the identity of the applicant based on the procedure of section 3.1.9, the RAO will print the certificate application with the registration authority counter system and will take out the printed IC card.

(2) The applicant will conduct confirmation on the certificate application and the printed IC card. If there is no error, the applicant shall sign the application and send back the IC card to RAO.

(3) Upon receipt of the signed and confirmed application, the RAO will utilize its IC card to sign the digital signature on the certificate application information

(4) The related certificate application information will be uploaded to the registration authority.

(5) Upon examination that there is no error on the signature of RAO, the registration authority will base on completed certificate application message to apply for certificate with the certificate authority.

(6) The certificate authority will resend the issued certificate and the issued certificate will be written on the IC card of the applicant through the registration authority counter system.

If the above issue examination is not passed, this authority will refuse issue of the certificate. The certificate applicant can be connected on-line to the repository to inquire on the certificate issue condition. This authority has the right to refuse issue of certificate to any entity. At the same time, to the certificate applicant who is refused with issue of certificate, this authority bears no damage indemnity liability.

4.3 Certificate acceptance procedure

After completing the issue of certificate, applicant can utilize one the following methods to conduct certificate acceptance operation depending on its requirement: one is at the counter and another is on-line method.

When conducting the counter method to accept the certificate, the registration authority counter will print out the certified IC card acceptance confirmation letter to the applicant. The applicant shall check the related

certificate content printed in the certified IC card acceptance confirmation letter. If the applicant confirms that the certificate content is correct, then the applicant shall accept the issued certificate and sign on the certified IC card acceptance confirmation letter expressing that the issued certificate is accepted.

When conducting the on-line method to accept the certificate, the registration authority counter system will display the certified IC acceptance confirmation message to the applicant. The applicant shall check the related certificate content in the certified IC card acceptance confirmation message. If the applicant confirms that the certificate content is correct, then the applicant shall click confirming acceptance of the issued certificate on the registration authority counter system.

Finally, based on the certified IC card certificate issue message of the applicant, the certificate acceptance procedure can be completed. Before signing the certificate acceptance message, the applicant shall decide on its own whether to announce its certificate. This authority will announce its certificate on the repository depending on the willingness of the subscriber. If the applicant discovers that the certificate content is incorrect, then the applicant shall refuse the acceptance of the certificate and shall reapply for certificate with the registration authority counter. In addition, if the mistake of the content of that certificate is caused by this authority or registration authority or registration authority window, then the registration authority counter will automatically reapply for certificate for the applicant. If the mistake is caused by the applicant, then the applicant will present reapplication of certificate.

Within ninety calendar days upon issue of the certificate, if the subscriber cannot complete the certificate acceptance operation, then it is deemed as refusal to accept certificate. That certificate will be automatically revoked and will not be announced.

4.4 Certificate temporary suspension and revocation

4.4.1 Cause of certificate revocation

Under the following conditions, the subscriber shall present certificate revocation application with the registration authority counter:

(1) When there is doubt or confirmation that the private key is being compromised.

(2) There is major alteration on the information recorded in the certificate

that can affect its reliability. For example, the name of the subscriber has been altered.

(3) Utilization of the certificate is no longer required.

This authority can conduct certificate revocation based on the following conditions without obtaining the consent of the subscriber in advance:

(1) Confirm that the content recorded in the certificate is incorrect.

(2) Confirm that the private key of the subscriber is fraudulently used, forged or compromised.

(3) Confirm that the private key of this authority is fraudulently used, forged or compromised that is sufficient to affect the reliability of the certificate.

(4) Confirm that the certificate of the subscriber is not issued according to the procedure provided in this statement.

(5) Confirm that the subscriber has violated the provision of this statement or related laws and regulations.

(6) According to the notification of official document of judicial authority.

(7) Death of the certificate subscriber or the death is declared.

(8) The certificate subscriber has lost the nationality of Republic of China.

(9) The certificate subscriber has conducted name alteration.

(10) Alteration in the national citizen identity card.

4.4.2 Certificate revocation applying person

There are the following two types of applicants for certificate revocation that is approved by this authority:

(1) Subscriber who intends to revoke the certificate.

(2) Judicial authority processed based on official document.

4.4.3 Certificate revocation procedure

Subscriber who intends to revoke the certificate shall process at the counter and shall provide the original of its national citizen identity card. Upon receipt of the certificate application information, the registration authority counter will conduct identity authentication procedure based on the provision of Chapter 3 of this standard so as to be the basis to judge whether the certificate revocation is agreed. Upon passing the examination of the certificate revocation application, the subscriber can be connected on-line to the repository to inquire on the certificate revocation condition.

If the judicial authority notifies specific certificate to be revoked based on official document, then this authority will revoke the certificate after examining the notifying official document.

If the above examination on the revocation application is not passed, this authority will refuse to revoke the certificate.

4.4.4 Certificate revocation application processing period

Starting from the time when the certificate revocation application is accepted at the registration authority counter, this authority will complete the certificate revocation processing procedure within one working day.

4.4.5 Cause of temporary suspension of certificate

Under the following two kinds of condition, the subscriber can apply for temporary suspension of certificate:

(1) When the token of the certificate key pair is lost or when it is being suspicious of being fraudulently used.

(2) Self-recognition that it is necessary to apply for temporary suspension of certificate.

This authority can base on the following condition to directly suspend the certificate temporary without prior consent from the subscriber:

(1) Based on the official document notification of the judicial authority.

4.4.6 Certificate temporary suspension applicant

The following two parties can be the certificate temporary suspension applicants:

(1) Subscriber who intends to suspend the certificate temporary.

(2) Judicial authority processed based on official document.

4.4.7 Certificate temporary suspension procedure

When subscriber who intends to suspend the certificate and process at the counter, such subscriber should present the original of its national citizen identity card. Upon receipt of the application for temporary suspension of certificate, the registration authority will confirm the identity of the subscriber based on the provision of section 3.1.9 of this statement so as to be the basis of judgment whether the temporary suspension of certificate can be agreed.

Subscriber can be connected on-line to the repository to apply for temporary suspension of certificate but the subscribe has to fill in the

subscriber password as the basis of identity certification. After the RAO has confirmed the identity of the subscriber, the RAO will present temporary suspension application to this authority on behalf of the subscriber and the subscribe code shall be reestablished.
If the above temporary suspension examination is not passed, this authority will refuse the temporary suspension certificate.

4.4.8 Certificate temporary suspension processing period and suspension period

Starting from the time of acceptance on the temporary suspension of certificate by the registration authority counter, this authority shall complete the certificate temporary suspension processing procedure within one working day.
During the application for temporary suspension of the certificate, the subscriber is not required to advise on the period required to be suspended. The longest time set for temporary suspension of certificate by this authority is the period from the time of the approval of application till that certificate is due.
During the period of temporary suspension of certificate, if the subscriber cancels the temporary suspension of certificate, then the subscriber shall complete restoration of the utilization of certificate and that certificate will be restored as valid.

4.4.9 Certificate revocation list issue frequency

The issue frequency of certificate revocation list is once a day and the updated certificate revocation list will be stored in the repository.

4.4.10 Certificate revocation list examination rules

When the relying party is utilizing the certificate revocation list announced by this authority in the repository, such party shall first check on its digital signature so as to confirm whether that certificate revocation list is correct. In regard to the essentials that should be possessed for conducting inquiry with the announced information in the repository by the relying party, please refer to the explanation in section 2.6.3.

4.4.11 On-line certification status inquiry service

This authority provides on-line certificate status (OCSP). For related explanation please refer to the repository.

4.4.12 On-line certification status inquiry provision

If the relying party cannot base on the provision of section 4.4.10 to inquire on the certificate revocation list, then it is necessary to utilize the inquiry service in section 4.4.11 to check whether the utilized certificate is valid.

4.4.13 Other revocation announcement form

Presently there is no provision of other form of revocation announcement.

4.4.14 Other revocation form announcement inspection provision

Presently there is no provision of other form of revocation announcement.

4.4.15 Other special provision when the key is compromised

To be processed based on the provision of section 4.4.1, 4.4.2 and 4.4.3.

4.5 Safety audit procedure

Safety related incidents of this authority should have safety audit log. The safety audit log will be generated in the form of system automatic generation, work record and papers etc. All audit logs will be properly kept and can be immediately acquired during execution of audit. For the maintenance of safety audit log, it will be processed based on the provision of archive retention period in section 4.6.2

4.5.1 Recorded event category

(1) Safety audit

- Any alteration in major audit parameters such as audit frequency, audit incident form, new and old parameter content.
- Any attempted deletion or revision audit log file.

(2) Identification and authentication

- Attempt the new role setting regardless of whether it is successful or failed
- Maximum endurance number of times of alteration of identity authentication attempt
- Maximum value of the number of times of failure in identity authentication attempt when the subscriber is log in to the system

- If the manager has unlocked the account number that has been locked and that account number is being locked due to multiple times of failed identity authentication attempt.
- The manager alters the identity authentication system of the system. For example, alteration from password to biological characteristic value.

(3) Key production

- When this authority is producing the key (not including production of key that is used in single time or only limited to one time use)

(4) Key load in and storage

- Load in the private key to the system component.
- All work in order to conduct key recovery and the access conducted on the private key kept in this authority.

(5) Addition, deletion and storage of reliable open key

- Alteration of reliable and public key including addition, deletion and storage.

(6) Export of private key

- Export of private key (not including the key of one time use or limited to one time use only).

(7) Certificate registration

- Certificate registration application course.

(8) Revoke the certificate

- Certificate revocation application course.

(9) Approval on alteration of certificate status

- Approve or refuse the application for alteration of certificate status.

(10) Configuration setting of this authority

- Alteration in the safety related configuration setting of this authority.

(11) Account number management

- Add or delete role and user.
- Revision on the access authority limit of the account number or role of the user.

(12) Management of analysis of certificate format

- Alteration in the analysis of the certificate format

(13) Management of the analysis on the certificate revocation list

- Alteration in the analysis of the certificate revocation list

(14) Others

- Install the operation system.
- Install the system of this authority.
- Install hardware cryptographic module.
- Remove hardware cryptographic module.
- Destroy hardware cryptographic module.
- Activate system.
- Attempt to log in the certificate management operation of this authority.
- Reception of hardware and software.
- Attempt to set the password.
- Attempt to revise the password.
- Internal information back up of this authority.
- Internal information recovery of this authority.
- Transmit any information to the repository for announcement.
- Access of internal database of this authority.
- Any announcement on compromise of certificate.
- Certificate load in token.
- Transmission of token.
- Zero value of token.
- Key alteration of this authority.

(15) Server setting alteration of this authority

- Hardware.
- Software.
- Operating system.
- Patches.

- Safety format analysis

(16) Substance access and site safety

- Equipment room entry and exit by personnel of this authority.
- Access from the server of this authority.
- Knowing or suspicious of violating the actual object safety provision.

(17) Abnormality

- Software error.
- Software inspection integrity failure.
- Receive inappropriate message.
- Abnormal route message.
- Network attack (suspicious or confirmed).
- Equipment breakdown.
- Improper electricity.
- Uninterrupted power supply (UPS) failure.
- Obvious and major network service or access failure.
- Violation of certification policy.
- Violation of this statement.
- Reset system clock.

4.5.2 Log file processing frequency

Every two months this authority will inspect the audit log one time to follow up and investigate on major incident. Inspection work includes certifying whether the audit log has been altered and inspecting all recorded items and any warning or abnormality. The result of the inspection audit log shall be recorded in documents.

4.5.3 Audit log file custodian period

The onsite audit information will be preserved for two months and shall be processed based on related provision of record preservation management system in section 4.5.4, 4.5.5 and 4.5.6.

If the preservation period of the audit log file is expired, the auditor is responsible for removing the information that cannot be carried out by other party on behalf.

4.5.4 Audit log file protection

(1) For utilizing signature and encryption technology to preserve the present and the filed audit log and for utilizing CD-R or other media storage that the audit log cannot be altered.
(2) The private key of the signature incident record can no longer be utilized in other usage and utilization of private key of the audit system for other is strictly prohibited. The audit system cannot leak out the private key.
(3) Manual audit log shall be kept in safe place.

4.5.5 Audit log file back up procedure

Electronic audit log will be back up once every month.

(1) This authority will conduct cyclic back up of incident and the audit system will conduct cyclic archive of audit track information daily, weekly and monthly.
(2) This authority will keep the incident record file in safe place.

4.5.6 Safety audit system

The audit system is built inside the system of this authority. The audit procedure will be activated when the system of this authority is activated and will stop only when the system of this authority is closed.
If the automatic audit system cannot function normally and when the safety system of simultaneous protection of the integrity and confidentiality of the system information is at a high-risk status, this authority will temporary suspend the certificate issue service and such service will be provided again until the problem is solved.

4.5.7 Advice on the incident

For recording by the audit system due to occurrence of incident, the audit system is not required to be advised that the incident caused by the entity of that incident has been recorded by the system.

4.5.8 Weak point evaluation

At least once a year, this authority will conduct weak point scanning on the certification management system and will conduct related reinforcement measures.

4.6 Record archive method

4.6.1 Recorded event category

(1) Accreditation information of this authority.
(2) Certification practice statement.
(3) Major contract.
(4) System and equipment configuration setting.
(5) System or configuration setting revision and update content.
(6) Certificate application information.
(7) Revocation application information.
(8) Certificate acceptance confirmation record.
(9) Token activation record.
(10) Issued or announced certificate.
(11) Key replacement record of this authority.
(12) Issued or announced certificate revocation list.
(13) Audit log.
(14) Other explanation information or application program utilized to certify and to serve as evidence for the archive content.
(15) Document required by the audit personnel.
(16) Organization and individual identity authentication information stipulated based on section 3.1.8 and 3.1.9.

4.6.2 Archive custody period

The custody period of the archive information of this authority is ten years. Application utilized in processing the archive information will also be maintained for ten years.

4.6.3 Archive protection

(1) Addition, revision or deletion on the archive information is not allowed.
(2) This authority can transfer the archive information to another storage media and shall provide adequate protection. The protection level shall not be lower than the original protection level.
(3) The archive information will be kept in a safe place.

4.6.4 Archive back up procedure

Back up of archive information to the support center of other place (refer to section 5.1.8.)

4.6.5 Time chop record requirement

Archive electronic record (such as certificate, certificate revocation list and audit log etc.) includes date and time information. In addition, these records will all go through adequate digital signature protection that can be utilized to check whether the date and time information of the inspection record is being altered.

However, the date and time information in the inspection record in this electronic record is not the electronic time chop information provided by a fair third party and instead it is the date and time of the computer operating system. All computer systems of this authority will conduct periodical time calibration so as to ensure the accuracy and reliability of the date and time information in the electronic record.

Archive of writing record will also record date information and if necessary, time information will also be recorded. The date and time record of the written record cannot be altered arbitrarily. If alteration is necessary, it has to be signed and confirmed by the audit personnel.

4.6.6 Archive information summarized system

This authority has no archive information summarized system.

4.6.7 Procedure for acquiring and certifying archive information

It is necessary to apply in writing to obtain official authorization before acquiring the archive information.

The auditor is responsible for certifying the archive information. For written document, it is necessary to certify the true and false of the signatory of the certified document and date. For electronic file, then digital signature of the archive information will be certified.

4.7 Key replacement

Private key of this authority will be replaced periodically based on the provision of section 6.3.2. Two months before the certificate is due, this authority will replace the key pair used to issue certificate. After the key pair is replaced, the authority will apply for new certificate with the government certificate management center.

Private key of the subscriber has to be replaced periodically based on the provision of section 6.3.2. If the utilization period of the private key of the subscriber is expired and replacement of key is required, it is necessary to apply for new certificate with this authority based on the provision of section 4.1.

4.8 Recovery procedure when the key is being compromised or during disaster

4.8.1 Computer resource, software or information damage recovery procedure

This authority stipulates the recovery procedure of computer resource, software and when information is being damaged and at the same time, exercise will be conducted every year.

If the computer equipment of this authority is being damaged or cannot be operated but the signature key of this authority has not yet been destroyed, then it is a priority to recover the operation of the repository of this authority and rebuild the ability of certificate issue and management as soon as possible.

4.8.2 Recovery procedure for the revocation of signature key certificate of the Ministry of the Interior Certification Authority

When the signature key certificate of this authority is revoked, this authority will generate key pair and will re-issue self signed certificate and certificates of all subscribers. In addition, all new certificates will be announced in the repository (not including certificates that subscribers have decided on their own on non-announcement) in order to announce or notify subscriber to alter the certificate.

4.8.3 Recovery procedure when the signature key certificate of the Ministry of the Interior Certification Authority is compromised

When there is worry on damage on the private key of this authority, this authority will generate key pair and will re-issue self signed certificate and certificates of all subscribers. In addition, all new certificates will be announced in the repository (not including certificates that subscribers decided on their own on non-announcement) in order to announce or notify subscriber to alteration the certificate.

4.8.4 Recovery work after the disaster of safety facilities of the Ministry of the Interior Certification Authority

This authority stipulates the recovery procedure after the disaster of the safety facilities and at the same time, exercise will be conducted every year. If there is occurrence of disaster, it is a priority to recover the operation of the repository of this authority and rebuild the ability of certificate issue and management as soon as possible.

4.9 Termination Service of the Ministry of Interior Certification Authority

When this authority terminates the service, it will be processed based on related provision of electronic signature law.

This authority shall abide by the following so as to ensure that the effect on the subscribers and relying parties due to termination of service can be at a minimum:

(1) Thirty days before the scheduled termination of service, this authority shall notify the competent authority of the electronic signature law (Ministry of Economic Affairs) and shall announce the fact of the service termination in the repository.

(2) When this authority terminates the service, the following measures will be adopted:

- Suspend the issue of new certificate.
- Terminate the certificate that is still valid at that time and continue to provide the service of certificate revocation list on the repository until the certificate validity period of all subscribers is due.
- The government will publicize various certification organizations of key infrastructure to undertake related business of various certification. If there is no appropriate certification organization that can undertake that type of certification, the competent authority of the electronic signature law will arrange other certification organization to undertake such certification.
- All record files during the operation period will be handed over to other certification organizations that undertake this business.
- If necessary, the competent authority of the electronic signature law can announce the certificate that is still valid at the time of revocation.

5. Non-technical safety control

5.1 Substance control

5.1.1 Substance location and structure

The equipment room of this authority is located in the information center of this Ministry and conforms to the government credit and equipment room facility standard of storage of high importance and sensitivity. In addition, it has substantial safety system including door security, security and surveillance tape recording etc. so as to prevent unauthorized access of related equipment of this authority.

5.1.2 Substance access

This authority operates based on the provision of assurance level 3 substance control. The equipment room has a total of four layers of door security. The first layer is all year round stationing security person. The second layer is floor card reader entry and exit control system. The third layer is the equipment room personnel finger print identification entry and exit control system. The finger identification device adopts three dimensional finger print sampling that can judge and identify the depth of the print and the color and whether it is a living body. The fourth layer is machine case intelligence card reader and the equipment room personnel is required to use the intelligence card in order to open the machine case.

Apart from restricting unrelated personnel to be near the equipment room by the door security system, the surveillance system of the machine case can control the opening of the machine case so as to prevent unauthorized access of related equipment including hardware, software and hardware cryptographic module.

To bring in any portable storage media into the equipment room, it is required to check and confirm there is no computer virus or any malicious software that can endanger the system of this authority.

Entry to and exit from the equipment room by person who is not the personnel of this authority is required to fill in the entry and exit record and related personnel of this authority should accompany such person in full course.

When related personnel of this authority leave the equipment room, it is required to conduct the following examination and recording so as to prevent entry into the equipment room by unauthorized personnel:

(1) Confirm whether the equipment can operate normally.
(2) Confirm whether the machine case door is locked.
(3) Confirm whether the door security system can operate normally.

5.1.3 Power and ventilation

The equipment room of this authority is equipped with independent constant temperature and constant humidity ventilation system so as to control the temperature and humidity of the environment so that the equipment room can maintain its best operation environment.

5.1.4 Flood prevention and protection

The equipment room of this authority is established at the third floor of

the building that is raised at the site. The partition of this building has water prevention facility and water pump.

5.1.5 Fire prevention and protection

The equipment room of this authority possesses automatic fire detection and warning function. The system can automatically activate the fire extinguishing equipment. In addition, manual switch is established at the main entrance and exit of various equipment rooms so that on-site personnel can activate manually during emergency.

5.1.6 Media storage

Audit log, archive and back up information storage media will be stored in the equipment room of this authority for one year. After one year, it will be moved to the back up site in an other place for storage.

5.1.7 Waste handling

For confidential information of this authority mentioned in section 2.8.1, when documentary information is not only required it will be processed by paper shredder. For magnetic tape, hard drive, floppy disk, magnetic optical disk (MO) and other form of memory, before reporting for waste, it will go through formatting procedure to remove the stored information and the CD will be destroyed.

5.1.8 Other place backup

The other place backup equipment room is away from this authority for over 30 kilometers that is sufficient to avoid damage on two places when disaster occurs. The backup content includes information and system program. All information backups will be executed at least once a week. The altered information backup will be executed on the day of alteration. The other place backup system and the system of this authority have the same safety level.

5.2 Procedure control

This authority is controlled by procedural controls in order to specify various trusted roles in the execution of related operation of the system and the number of people required for each job and the identification and authentication of each role so as to ensure the safety of the system operation procedure.

5.2.1 Trusted role

In order to execute the responsibility of related operation of the system and to be able to conduct appropriate distinction so as to avoid malicious utilization of the system by certain people without being noticed, for the access operation of each system, this authority clearly specifies which trusted role can execute this operation.

This authority has five different types of trusted roles that are administrator, officer, auditor, operation and controller respectively. Each type of trusted role will conduct control on personnel based on the provision of section 5.3 so as to prevent possible internal attack. Each type of trusted role can be undertaken by many people and for each type of trusted role there will be one chief role. The work content of the five types of trusted role is explained as follows:

(1) The administrator is responsible for

- Install, set and maintain the system of this authority.
- Establish and maintain the account number of the subscriber of this authority system.
- Set audit parameters.
- Produce and make back up of the key of this authority.

(2) The officer is responsible for

- Activate or suspend the certificate issue service.
- Activate or suspend the certificate revocation service.

(3) The auditor is responsible for

- Examination, maintenance and archive of the audit log.
- Execute or supervise internal audit so as to confirm whether this authority can abide by the provision of this statement.

(4) The operator is responsible for

- Daily operation and maintenance of the system equipment.
- System backup and recovery operation.
- Storage media update.
- Software and hardware update except for the certificate management system of this authority.
- Network and website maintenance : establish system safety and virus

protection system and network safety incident detection and reporting etc.

(5) The controller is responsible for:

■ Safety control of the system (such as the door security management of the equipment room, fire prevention, water prevention and ventilation system etc.).

5.2.2 Role allocation

Based on the five types of trusted roles defined in section 5.2.1, the role allocation of this authority is required to conform to the following provision:

(1) The three types of trusted roles including the administrator, officer and auditor cannot be undertaken concurrently. However, they can be operator concurrently.

(2) The controller cannot take up other four types of roles concurrently.

(3) Any one type of trusted role is not permitted to execute self-audit function.

5.2.3 Number of persons required for each mission

According to the operation safety requirement of various types of trusted roles, the number of people required is as follows:

(1) Administrator : at least to be undertaken by three qualified persons.

(2) Officer: at least to be undertaken by three qualified persons.

(3) Auditor: at least to be undertaken by two qualified persons.

(4) Operator: at least to be undertaken by two qualified persons.

(5) Controller: at least to be undertaken by three qualified persons.

Number of people required for each mission is explained as follows:

Mission name	Administrator	Officer	Auditor	Operator	Controller
Install, set and maintain the management system of this authority	2				1
Establish and maintain the user account number of the certification management system of this authority	2				1
Set the audit parameters	2				1

Produce and back up the key of this authority	2		1		1
Activate or suspend the certificate issue service		2			1
Activate or suspend the certificate revocation service		2			1
Examination, maintenance and archive of audit log			1		1
System equipment daily operation and maintenance				1	1
System back up and recovery operation				1	1
Storage media update				1	1
Software and hardware update apart from the certification management system of this authority				1	1
Network and website maintenance				1	1
Set the safety control of the system					2

5.2.4 Identify and authenticate each role

The authority utilizes the account number of users, password and the system account number management function group and IC card to identify and authenticate different roles of the administrator, officer, auditor and operator etc. In addition, the authority limit setting function of the central door security system is utilized to identify and authenticate the safety controller.

5.3 Personnel control

5.3.1 Family background, qualification, experience and safety requirement

(1) Employee selection and employment safety evaluation

- ■ Personal character evaluation.
- ■ Evaluation on the work experience of the applicant
- ■ Academic, professional ability and qualification evaluation.
- ■ Personnel identity confirmation.
- ■ Personnel conduct evaluation.

(2) Personnel examination management

Before employing related personnel, this authority will conduct qualification examination first so as to confirm its qualification and work ability. After official employment, employee is required to accept educational training. In addition, based the responsibility to be borne signed in writing, qualification repeat examination will be conducted every year. If the employee cannot pass the qualification repeat examination, then he/she will be transfered from the present job and other qualified person will be dispatched to undertake such job.

(3) Employment and dismissal of personnel and transfer management

If there is alteration in the employment of personnel, employment terms or contract, especially when the employee departs from the employment or when the employment contract expires, such personnel should abide by the agreement to maintain the confidentiality responsibility.

(4) Agreement on maintaining the confidentiality responsibility.

Related personnel of this authority shall bear the responsibility of confidentiality maintenance and shall sign the confidentiality preservation guarantee and cannot disclose secret in the form of verbal, photocopy, borrowing for reading, handing over, essay publishing or other method.

5.3.2 Family background examination procedure

For all types of trusted role personnel mentioned in section 5.2.1, before their employment, this authority will conduct qualification examination so as to confirm whether related certifying documents of their identity qualifications are correct.

5.3.3 Education training requirement

Trusted role	Educational training requirement

Administrator	1. Safety certification of this authority. 2. Operation procedure of installation, setting and maintenance of this authority. 3. Operation procedure for establishing and maintaining the subscriber account number of the system. 4. Operation procedure for setting the audit parameters. 5. Operation procedure for producing and making back up of the key of the authority. 6. Procedure for recovery after disaster and business sustainable operation.
Officer	1. Safety certification system of this authority. 2. Utilization and operation procedure of software and hardware of the system of this authority. 3. Certificate issue operation procedure. 4. Certificate revocation operation procedure. 5. Procedure for recovery after disaster and business sustainable operation.
Auditor	1. Safety certification system of this authority. 2. Utilization and operation procedure of software and hardware of the system of this authority. 3. Operation procedure for producing and making back up of the key of this authority. 4. Operation of examination, maintenance and archive of audit log. 5. Procedure for recovery after disaster and business sustainable operation.
Operator	1. Safety certification system of this authority. 2. Maintenance procedure of the daily operation of the system equipment. 3. Update procedure of storage media. 4. Procedure for recovery after disaster and business sustainable operation. 5. Network and website maintenance procedure.
Controller	1. Setting of the door security authority limit procedure. 2. Procedure for recovery after disaster and business sustainable operation.

5.3.4 Personnel re-education training requirement and frequency

During software and hardware upgrade, work procedure alteration,

equipment replacement or alterations in related regulations, this authority will arrange related personnel to conduct re-education training and will record the training condition so as to correctly understand the alterations in related operation procedure and regulations.

5.3.5 Work transfer frequency and sequence

(1) After the administrator has been transferred from the original post for one full year, such person can then be appointed as officer or auditor.

(2) After the officer has been transferred from the original post for one full year, such person can then be appointed as administrator or auditor.

(3) After the auditor has been transferred from the original post for one full year, such person can then be appointed as administrator or auditor.

(4) After an operator has worked for a full two years and has accepted related education training and has passed the examination, such person can be appointed as administrator, officer and auditor.

5.3.6 Suppression of unauthorized action

If related personnel of this authority violates the certification policy and this statement or other procedure announced by this authority, such person will accept appropriate management and reprimand. If the condition is major resulting in damage, then legal action will be taken to seek for its responsibility.

5.3.7 Personnel employment provision

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

5.3.8 Provided documentary information

This authority will provide related documents including the infrastructure certification policy, technical standard, this statement, system operation manual and electronic signature law etc. to related personnel of this authority.

6. Technical safety control and management

6.1 Key pair production and installation

6.1.1 Key pair production

Based on the provision of section 6.2.1, this authority will produce key pair within the software cryptographic module and will adopt true random number generator and RSA key calculation method. After the production of private key within the hardware cryptographic module, it will be stored there all along and will not be leaked out.

For the production of the key of this authority, under witness by the Electronic Certification Steering Group Member of this Ministry and related personnel, it will be conducted by multiple person safety control system.

The token utilized by the subscriber is IC card. For its key pair, after the card management center has driven the IC with the safety control system, it will be produced on its own within the IC card. In addition, after the key pair production is completed, its private key cannot be transmitted from the IC card.

6.1.2 Safety transmission of private key to subscriber

After this authority has issued the certificate, the RAO will hand over the IC card stored with the private key to the subscriber.

6.1.3 Safety transmission of public key to the Ministry of Interior Certification Authority

From the registration authority counter, the public key of the subscriber will be transmitted to this authority via safety channel.

The safety channel in this section refers to the information encryption transmission method by utilizing the secure socket layer 129bits or other similar or even higher level.

6.1.4 Safety transmission of public key of the Ministry of Interior Certification Authority to relying parties

The public key certificate of this authority itself is issued by the government certification chief authority that is announced in the repository of the government certification chief authority. Relying parties can download directly and utilize. Before utilizing the public key certificate of this authority, the relying party has to base on the provision of the certification practice standard of the government certification chief authority to acquire the public key or self signed certificate from the government certification chief authority via safety channel. Then the

signature on the public key certificate of this authority issued by the government certification chief authority will be examined so as to ensure that the public key of the public key certification can be trusted.

6.1.5 Key length

This authority utilizes 2048 bits RSA key and SHA-1 mixed function calculation method to issue certificate and subscribers utilizes 1024 bits RSA key.

6.1.6 Key parameter production

The public key parameter of the RSA calculation method adopted is Null.

6.1.7 Key parameter quality inspection

This authority adopts ANSI X0.31 calculation method to generate the prime number required by RSA calculation method. That method can guarantee that the prime number is strong prime.

Subscriber's key can generate the required prime number in the RSA calculation method inside the IC card or other software and hardware cryptographic module. However, it is not guaranteed that such prime number is strong prime.

6.1.8 Key produced through software or hardware

Based on the provision of section 6.2.1, this authority will utilize the random number produced by hardware cryptographic module, pubic key pair and corresponding key.

According to the provision of section 6.2.1, the card management center will utilize the key pair of the subscriber produced by the IC card hardware cryptographic module.

6.1.9 Key utilization purpose

The public key certificate of this authority itself is issued by the government certification chief authority. Amongst this, the certification key usage extension sets that the key usage bit is keyCertSign and cRLs sign. The signature private key of this authority will only be utilized in the issue of certificate and certificate revocation list.

Subscriber certificate includes two pairs of key pairs for signature use and encryption use.

6.2 Private key protection

6.2.1 Key module standard

In order to conform to the provision of certification policy section 6.2.1 assurance level 3, this authority utilizes safety level 3 standalone hardware cryptographic module. The subscriber utilizes safety level 2 IC card hardware cryptographic module.

In addition, the standalone hardware cryptographic module utilized by this authority has safety evidential information and the IC card utilized by subscriber is information that can be serving as evidence.

6.2.2 Key separate possession control and management by multiple persons

The multiple person control of separate holding of key of this authority adopts Shamirs' Secret Sharing m-out-of-n (hereinafter abbreviated as m-out-of-n). This is a kind of secret sharing method that has perfect secret and can be the method for private key separate holding back up and recovery. By adopting this method, it can allow that multiple person control of private key of this authority has maximum safety. Therefore it is also utilized to be the activation method of private key (refer to section 6.2.7).

6.2.3 Private key escrow

The signature private key of this authority cannot be escrowed and this authority is not responsible for keeping the signature private key of subscriber.

6.2.4 Private key back up

The multiple person control method of key separate holding in section 6.2.2 is utilized to make back up of private key and the IC card with high safety and is utilized as the storage media of secret separate holding.

6.2.5 Private key archive

This signature secret key of this authority cannot be archived. This authority will not conduct archive on the signature private key of subscribers.

6.2.6 Input of private key to cryptographic module

This authority will only input the private key into the cryptographic

module when conducting recovery of the key back up.

6.2.7 Private key activation method

The activation of the RSA private key of this authority is based on the m-out-of-n control IC card group to conduct control. Control IC card groups of different usage are separately kept by the administrator and the officer.

6.2.8 Private key suspension method

The suspension of the RSA private key of this authority is controlled based on the manual method of multiple person authorization control.

6.2.9 Private key destruction method

In order to avoid theft of the old private key of this authority center thus affecting the accuracy of the issued certificate, when the life of the private key of this authority is expired, it will be destroyed. Therefore, after this authority has completed the key update and issue of new certificate, the memory address of the old private key stored in the hardware cryptographic module is filled with zero (zerorization) so as to destroy the private key of the hardware cryptographic module. At the same time, separate holding of the old private key will conduct substantial destruction.

6.3 Other provision of management on subscriber's key

User has to manage the key pair on its own and this authority is not responsible for keep the private key of subscriber.

6.3.1 Archive of public key

This authority will conduct archive of certificates and will execute safety control of archive system based on the provision of section 4.6 and will not conduct archive of public key separately.

6.3.2 Utilization time limit of public key and private key

6.3.3.1 Utilization time limit of the public key and private key of the Ministry of the Interior Certification Authority

The key length of the public key and private key of this authority is RSA 2048 bits. The maximum utilization time limit of public key certificate is twenty years and the maximum utilization time limit of

private key is ten years.

6.3.3.2 Utilization time limit of the public key and private key of subscriber

The key length of the public key and private key of subscribe is RSA 1024 bits. The maximum utilization time limit of public key certificate is five years and the maximum utilization time limit of private key is five years.

6.4 Activating information protection

6.4.1 Activating generation of information

Information activation of this authority is generated from the hardware cryptographic module that will be written into the m-out-of-n control IC card group. The activated information in the IC card will be directly accessed from the card reader built inside the hardware cryptographic module. The PIN number of the IC card will be input directly from the keyboard built inside the hardware cryptographic module.

6.4.2 Activating information protection

The activated information of this authority is protected by m-out-of-n control IC card group. The custody personnel are responsible for the custody of the PIN number of the IC card. If the number of failure of log in is more than three times, then this IC card will be locked. When the IC card is being handed over, the new custodian is required to re-set new PIN number.

6.4.3 Other activating information provisions

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

6.5 Computer software and hardware safety control measures

6.5.1 Specific computer safety technology requirement

This authority and other related subsidiary system would go through the operation system or cooperate with the operating system and the protection measures of software and hardware to provide the following safety control functions:

(1) Possesses identity authentication log in.

(2) Provides discretionary access control.

(3) Provides safety audit ability.
(4) Restraints on various types of certification service and trusted role access control.
(5) Possesses identification and authentication of trusted role and identity.
(6) Possesses safe and reliable channels of trusted role and related identity role.
(7) Possesses procedure integrity and safety control protection.

6.5.2 Computer safety rating

This authority adopts safety strength and computer operation system equivalent to Trusted Computer System Criteria (TCSEC).

6.6 Life cycle technology control and management measures

6.6.1 System research and development, control and management measures

The system research and development of this authority follows the ISO9001 standard to conduct quality control.

The hardware and software of this authority is exclusive that can only utilize components with safety authorization. There is no installation and operation of unrelated hardware installation, network connection or component software. In addition, there will be automatic daily inspection to check whether there is any malicious program code.

6.6.2 Safety management control and management measures

During the first time installation of software, this authority will confirm that the supplier provides accurate edition that has not yet been revised. After the system is installed, this authority will automatically check the integrity of the software every day.

This authority will record and control the configuration of the system and any revision and function enhancement, at the same time, this authority will detect any revised system software or configuration that has not yet been permitted.

6.6.3 Life cycle safety rating

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 safety control and management measures

Through double firewall the mainframe and the internal repository of this authority connects with the external network. The external repository is established in the external service area of the external firewall (non-military zone DMZ) and is connected to the Internet. Apart from necessary maintenance and backup, it will provide uninterrupted certificate and certificate revocation list inquiry service.

The internal repository information of this authority (including certificate and certificate revocation list) is protected by digital signature and is transmitted to the external repository from the internal repository automatically.

The external repository of this authority is protected through update of the system repair program, system weak point scanning, attack detection system, firewall system and filtering router etc. so as to protect blocking and attack etc.

6.8 Cryptographic module safety control measures

Refer to the provision of section 6.1 and 6.2 for its processing.

7. Format analysis

7.1 Certification format analysis

The format analysis of the certified issued by this authority is based on the related provision of this infrastructure technical standard.

7.1.1 Edition serial number

X.509v3 edition certificate issued by this authority.

7.1.2 Certificate extensions

The certificate extensions of the certificate issued by this authority is based on related provision of this infrastructure technical standard.

7.1.3 Calculation method for the object identification code

The calculation method for the object identification code of the signature of the certificate issued by this authority is:

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

(OID : 1.2.840.113549.1.15)

The calculation method for the object identification code of the subject public key of the certificate issued by this authority is:

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

(OID : 1.2.840.113549.1.1.1)

7.1.4 Naming form

The two column value of the subject of the certificate and the officer utilize the only identification name of X.500. The attribute form of this name follows the related provision of RFC 3280.

7.1.5 Naming constraint

The certificate issued by this authorize does not utilize nameConstraints.

7.1.6 Certification policy on object identification code

The certification policy on object identification code of this infrastructure is utilized.

7.1.7 Utilization of policy constraints extensions

The certificate issued by this authority does not utilize policyConstraint extensions.

7.1.8 Language method and language meaning of policy constraint

The certificate issued by this authority does not include policyQualifiers.

7.1.9 Word meaning processing of critical certification policy extensions

The certification extensions included in the certificate issued by this authority will not be marked as key extensions.

7.2 Certification revocation list format analysis

7.2.1 Edition serial number

This authority issues X.509v2 edition certificate revocation list.

7.2.2 Certificate revocation list extensions

Certificate revocation list issued by this authority is based on related provision of this infrastructure technical standard.

8. Certification practice statement maintenance

8.1 Alteration procedure

This standard will be evaluated periodically every year on whether revision is

necessary so as to maintain its guarantee level. Revision methods include revision in the form of appended document and direct revision on the content of this statement. If there is revision on the certification policy or alteration in the object identification code, this statement will cope with the revision.

8.1.1 Alteration items during alteration that shall not be notified separately

When this statement is conducting new typesetting, there will be no separate notice.

8.1.2 Alteration items that should be notified

8.1.2.1 Alteration items

Evaluate the level of effect on the subscribers or relying parties by the alteration items:

(1) If the level of effect is large, revision will only be conducted after announcement for thirty calendar days in the repository of this authority.

(2) If the level of effect is little, revision will only be conducted after announcement for fifteen calendar days in the repository of this authority.

8.1.2.2 Notification system

All alteration items will be announced in the repository of this authority.

8.1.2.3 Reply time limit for opinion

If there is opinion on the alteration items, its reply time limit is:

(1) If the level effect of section 8.1.2.1 is large, the reply time limit is within fifteen calendar days starting from the day of announcement.

(2) If the level effect of section 8.1.2.1 is little, the reply time limit is within seven calendar days starting from the day of announcement.

8.1.2.4 System for handling opinion

If there is opinion on alteration items, before the opinion reply deadline is due, such opinion should be transmitted to this authority based on the reply method announced in the repository of this authority. This authority will consider such related opinion and will evaluate the alteration item.

8.1.2.5 Final announcement time limit

The announcement of alteration item of this standard shall be revised based on the provision of section 8.1.2.2 and 8.1.2.3. According to the provision of section 8.1.2.1, the announcement time limit is at least fifteen days of announcement until revision of this standard is effective.

8.2 Announcement and notification provision

Revision on this statement will be announced in the repository of this authority within seven calendar days. Unless otherwise provided, the effective day for the revision of this standard shall be effective during its announcement.

8.3 Certification practice statement examination procedure

After this statement is approved by the competent authority of the Electronic Signature Law, the Ministry of Economic Affairs, this authority will conduct announcement. After the announcement of revision on the certification policy, this statement will cope with the revision and shall send to the competent authority of the Electronic Signature Law, the Ministry of Economic Affairs for approval.

After the revision on this statement becomes effective, unless otherwise provided, if the content of the revision of this statement contravenes with the original statement, then it shall base on the content of the revised standard as standard. If the revision is conducted in the form of appended document and the content of that appended document contravenes with the original statement, then it shall base on the content of the appended statement as standard.