Ministry of the Interior Certificate Authority Certification Practice Statement

Version 2.0

Organizer: Ministry of the Interior

19, Nov. , 2021

Version Revision History

Version	Effective Date	Description of Revision
1.0	2003-04-03	Promulgation of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.0.
1.1	2003-09-18	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.1.
1.2	2005-06-17	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.2.
1.3	2008-02-29	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.3.
1.4	2010-11-19	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version1.4.
1.5	2011-08-19	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.5.
1.6	2013-06-11	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.6.
1.7	2014-08-04	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.7.
1.8	2015-08-25	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.8.
1.9	2016-02-01	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.9.
1.91	2019-02-20	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 1.91.
2.0	2021-11-19	Amendment of “Ministry of the Interior Certificate Authority Certification Practice Statement”, Version 2.0.

Table of Contents

Summary

According to the regulations of the certification practice statement based on electronic signature act authorized and promulgated by the Ministry of Economic Affairs, the important matters of the Ministry of the Interior Certificate Authority Certification Practice Statement (hereinafter referred to as “this Statement”) are described below:

1. Competent Authority’s Approval Doc. No.: Jing Shang Zi No. 11002437370.

2. Issued Certificate:

(1) Types: natural person public key certificate

(2) Assurance Level: Ministry of the Interior Certificate Authority (hereinafter referred to as “Certificate Authority”) operates at Level 3 of the assurance level of the Government Agency Public Key Infrastructure Certificate Policy (hereinafter referred to as “Certificate Policy”) and issues a certificate used for signature and encryption at Level 3 of the assurance level defined by the certificate policy.

(3) Scope of Applicability and Limit of Use: The issued certificate is applicable to identity recognition, digital signature and data protection in the network. Subscribers and relying parties shall use the certificate issued by the Certificate Authority and pay attention to the limit of the scope of applicability of this Statement.

3. Third Party Audit of Verification Service:

Certificate Authority receives two third party audits yearly: one of the audits is an annual external audit of the whole verification service through the GPKI Certificate Authority of National Development Council, and the other one is an evaluation of the information security management system through the ISO27001:2013 evaluation. Please refer to the website https://moica.nat.gov.tw/bs.html for the latest third-party audit result.

4. Legal Responsibility and Important Matters:

(1) The Certificate Authority shall not assume any legal responsibility for the consequence caused by the subscriber or relying party who has not used the certificate in accordance with the scope of applicability specified by this Statement.

(2) If a subscriber or relying party uses a certificate leading to the occurrence of an event that requires a compensation of loss or damage, and the damage is attributable to the Certificate Authority or its personnel who fails to handle the subscriber registration, certificate issuance or deactivation, revocation operation according to the related regulations of this Statement, the Certificate Authority will compensate the subscriber or relying party with the direct damage caused by the certification within the scope of compensation as specified in Section 2.2.1.4, but excluding indirect damages.

(3) The Certificate Authority shall not be liable for any damage caused by force majeure and other reasons not attributable to the Certificate Authority.

(4) The Certificate Authority will bear the legal responsibility arisen from the execution of business of the Registration Authority, Registration Authority Counter, or card management center, unless otherwise regulated by law.

(5) If a subscriber has concealed the facts and provided incorrect data to the Registration Authority Counter, leading to damages to the relying party, and such damages are not attributable to the Registration Authority Counter, the subscriber shall be liable to the damages.

(6) If it is necessary to suspend, reactivate, or revoke the subscriber's certificate, the suspension, reactivation or revocation shall be handled in accordance with the related regulations of this Statement.

5. Other Important Matters:

(1) If part of the certificate service needs to be suspended for the maintenance, conversion and expansion of the Certificate Authority's system, it shall be announced in the repository to notify the subscribers, but the subscribers or relying parties shall not use this as a reason to claim the Certificate Authority for the compensation of loss or damage. \

(2) When the Certificate Authority issues a certificate according to the subscriber's application, and the subscriber comes to the counter to receive the certificate, or when the subscriber completes the online confirmation and agrees to accept it, it means that the subscriber accepts the certificate issued by the Certificate Authority. The subscriber shall use the certificate according to the related regulation of this Statement. If the content or information of the certificate is wrong, the subscriber should proactively notify the Certificate Authority.

(3) The subscriber and relying party shall carefully select a safe computer environment and a trustworthy application system, the subscriber and relying party shall bear their own responsibility for damage caused by the factors of the computer environment or the application system.

(4) If the Certificate Authority fails to operate normally, the subscriber and relying party shall find another way to complete

the legal actions that should be done with others as soon as possible, and cannot use the failure to operate normally as a reason for defend against others. When a third party claims or requests the Certificate Authority for any liability, the subscriber and relying party shall be responsible for the liability for the damage to the Certificate Authority, and the compensation of damage is limited to direct damage to the Certificate Authority, but does not include indirect damage.

(5) When the relying party receives the certificate issued by the Certificate Authority, it means that the relying party has understand and agreed the clauses related to the Certificate Authority's legal responsibility, and will use the certificate in accordance with the related regulation of this Statement.

1 Introduction

Ministry of the Interior Certificate Authority Certification Practice Statement (hereinafter referred to as this Statement) is established according to the Certificate Policy for the Government Public Key Infrastructure (hereinafter referred to as "Certificate Policy") and follows the electronic signature act, specification of the certification practice statement, and related regulation, describing how the Ministry of the Interior Certificate Authority (MOICA), hereinafter referred to as "Certificate Authority") follows the regulation of Level 3 of the assurance level of the certificate policy to issue and manage the natural person public key certificate (hereinafter referred to as "Certificate").

1.1 Overview

According to the regulations of the certificate policy, the Certificate Authority is the first level subordinate certificate authority (Level 1 Subordinate CA) of the Government Public Key Infrastructure (GPKI, hereinafter referred to as this "Infrastructure"), responsible for issuing and managing MOICA certificates including two types of certificates used for signature and encryption respectively, and both of which are certificates of Level 3 of the assurance level of the certificate policy.

In this Statement, the certification practice of the Certificate Authority will be described to ensure that the Certificate Authority's certificate issuance and management comply with the regulations specified in Level 3 of the assurance level of the certificate policy. The practice operation specification stated in this Statement is only applicable to the Certificate Authority related individual including the Certificate Authority, Registration Authority, Registration Authority Counter, Card Management Center, Subscriber, Relying Party, Repository, etc.

The Ministry of the Interior (hereinafter referred to as "MOI") is a competent authority of the Certificate Authority, which is responsible for the establishment and amendment of this Statement, and this Statement

shall be promulgated and implanted after the approval by a competent authority of the Ministry of Economic Affairs and the electronic signature act. If this Statement is used by an unauthorized certificate authority other than the Certificate Authority, the unauthorized certificate organization shall be responsible for any problem caused by quoting and or using this Statement.

1.2 Document Name and Recognition

Document Name: Ministry of the Interior Certificate Authority Certification Practice Statement
Version: 2.0
Release Date: 19, Nov., 2021
Release Website: https://moica.nat.gov.tw/law_1.html.
Certificate Policy Object Identifier (CPOID): id-tw-gpki-certpolicy-class3Assurance, { id-tw-gpki-certpolicy 3}

1.3 Main Members

Related members participating in the verification service of this Statement include:

(1) Certificate Authority.

(2) Registration Authority.

(3) Registration Authority Counter.

(4) Card Management Center.

(5) Repository.

(6) End Entity.

1.3.1 This Management Center

The Certificate Authority is the Level 1 subordinate certificate

authority in this infrastructure, and complies with the regulation of Level 3 of the assurance level of the certificate policy, and is responsible for issuance and management operations of the MOICA certificate.

1.3.2 Registration Authority

The Certificate Authority will set up a Registration Authority, responsible for collecting and verifying the identity of a subscriber and registering of the certificate related information. The Registration Authority is composed of a multiple of Registration Authority Counters (RA Counters).

The Registration Authority has a Registration Authority server (RA Server) responsible for verifying the identity of a Registration Authority Officer (RA Officer, hereinafter referred to as "RAO") and managing the Registration Authority Counter. The Registration Authority Server is managed by the Registration Authority Administrator (RA Administrator) and responsible for management, and the Registration Authority Administrator sets a RAO account and authority on the Registration Authority server, and manufactures and issues a RAO IC card. The Registration Authority Server has the Registration Authority's private key, and communicates with the private key, and the Registration Authority Server and the Certificate Authority Server are protected by the signature of the Registration Authority's private key.

1.3.3 Registration Authority Counter

The Registration Authority Counter can be set up in the Household Registration Office of each municipality, county (city), the Immigration Agency of this Ministry, the service station of each county (city), or an organization authorized and approved by the Certificate Authority. The Registration Authority Counter may be set up in a temporary mobile location as needed, in addition to the Household Registration Office or the authorized organization.

The RAO of the Registration Authority Counter is responsible for the

operation of the Registration Authority Counter and accepts and handles the certificate registration operation approved by the Registration Authority Counter, such as the registration application, suspension application, reactivation application and revocation application of the certificate.

1.3.4 Card Management Center

The token of the key pair of the subscriber certificate shall comply with Section 6.2.1 of the specification. The Certificate Authority will entrust a trusted card management center for the token production and management operation. The token production and management operation include the internal production of the key pair of the token, and a random number is provided for setting the initial personal identifier (hereinafter referred to as "PIN code") and managing the delivery of the token.

1.3.5 Subscriber

The Certificate Authority's subscriber refers to natural person individual recorded in the certificate subject name of the certificate issued by the Certificate Authority.

1.3.6 Relying Party

Relying party refers to an individual who trusts the linking relationship between the certificate subject name and the public key.

Before the relying party uses the certificate issued by the Certificate Authority, it is necessary to check the validity of the certificate to be used according to the Certificate Authority. The certificate can be used for the following operations only if the validity of the certificate has been confirmed:

(1) Checking the integrity of the electronic document.

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

(3) Establishing a safe communication channel between the certificate subjects

1.3.7 Other Related Members

Chunghwa Telecom Co., Ltd. accepts the commission of this Ministry, and takes the responsibility of maintaining the system operation of this Management Center.

1.4 Usage of Certificate

1.4.1 Scope of Applicability of Certificate

The type of certificate issued and managed by the Certificate Authority is MOICA certificates, including the certificates used for signature and encryption.

The certificate issued by the Certificate Authority complies with the regulation of Level 3 of the assurance level of the certificate policy, and this certificate is applicable for the identity recognition, digital signature and data protection in networks.

1.4.2 Limit of Use of Certificate

When using the private key, the subscriber should carefully select a safe computer environment and a trustworthy application system to avoid the private key from being stolen or misused by malicious software and hardware and causing damage to rights.

Before using the certificate issued by the Certificate Authority, the relying party should confirm whether the type of the certificate, the assurance level and the usage of key usage meet the application requirements.

The relying party should handle the critical and non-critical certificate

extension fields in the certificate in accordance with the X.509 specification.

Before using the verification service provided by the Certificate Authority, the relying party shall carefully read and follow the regulations of this Statement, and shall pay attention to the amendment of this Statement at the same time.

1.4.3 Scope of Prohibited Use of Certificate

1. Crime.
2. Military order, war situation, and control of nuclear, biological and chemical weapons.
3. Nuclear operating equipment.
4. Aviation flight and control system.

1.5 Contact Method

1.5.1 Certification Practice Standard of Establishing and Managing Organization

The Certificate Authority is responsible for establishing each article of this Statement. The establishment and amendment of this Statement will be promulgated and implemented after the approval by the competent authority of electronic signature act of the Ministry of Economic Affairs.

1.5.2 Contact Information

Should there be any suggestion to this Statement, or any leakage missing of the private key data, please contact the Certificate Authority by the contact method as shown in the website https://moica.nat.gov.tw/.

1.5.3 Approval of Certification Practice Statement

According to the related regulations of the electronic signature act related, this Statement must be approved by the act competent authority of the electronic signature of the Ministry of Economic Affairs before

providing the certificate issuance service.

1.5.4 Certification Practice Statement Modification Procedure

The modification of certification practice statement shall be handled according to the regulations of Section 1.5.3 “Approval of Certification Practice Statement”. If there is an amendment of the certificate policy which has be published, this Statement should cooperate with the amendment.

1.6 Definition and Abbreviation of Terms

Refer to Appendix 1 for “glossary” and Appendix 2 for “Abbreviation of English Terms”.

2 Release of Information and Responsibility of Repository

2.1 Repository

The repository shall announce the information as follows:

(1) Related information of the issued certificate, certificate revocation list and other certificate.

(2) Certificate policy and this Statement.

(3) Latest external audit result.

(4) This management center's certificate (all certificates released to the expiry date of the certificate duration issued by the private key corresponding to the public key of the certificate).

The repository provides 24-hour service, and related information is published in the website: "https://moica.nat.gov.tw/".

The access control of the repository is handled in accordance with the regulation as specified in Section 2.4 "Access Control".

2.2 Release of Certificate Information

This management center adopts the following method to release the certificate information:

1. Certificate Revocation List (CRL).
2. Providing Online Certificate Status Protocol (OCSP) inquiry service.
3. Certificate inquiry service of the repository.

2.3 Announcing Frequency or Time

1. This Statement is announced after the approval by the competent authority and amended in accordance with the regulations of Chapter 8.
2. The Certificate Authority issues the certificate revocation list once a day and the certificate revocation list is announced in the repository.
3. The Certificate Authority's certificate is announced in the repository upon issuance.

4. The issued certificate is announced in the repository upon issuance.
5. The certificate policy is announced after the approval by the electronic government authority, and subsequent amendment is announced in accordance with the regulation as specified in Chapter 8 of the certificate policy.
6. The number of days described in this certification practice statement will be calculated in terms of "calendar days" if not specifically marked as "working days".

2.4 Access Control

The Certificate Authority' host is built inside a firewall, and cannot be connected directly from the outside. The repository host is controlled the firewall system and connected to the database of the Certificate Authority's host to retrieve certificate information or download certificate.

Information published by the Certificate Authority in accordance with Section 2.2 is mainly provided for query by subscribers or relying parties, so that it is opened and provided for reading and access. Access control should be taken to ensure the security of the repository, and the access status and availability should be maintained.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Naming

The certificate subject name of the certificate issued by the Certificate Authority adopts a X.500 distinguished name (DN).

3.1.2 Naming Must be Meaningful

The Certificate Authority mainly adopts the Chinese name stored in the database of the Household Registration Office, MOI system for subscribers of this country, and mainly adopts the Chinese or English name stored in the Entry, Exit and Immigration Agency Business Management System stored in the Immigration Agency, MOI for non-resident subscribers.

3.1.3 Subscriber's Anonym or Pseudonym

This management center does not issue an anonymous certificate or pseudonymous certificate.

3.1.4 Rules of Interpreting a Naming Form

According to the format profile of the certificate in the technical specification of this infrastructure, the rule of interpreting various naming forms is defined according to the ITU-T X.520 name attributes.

3.1.5 Uniqueness of Naming

The Certificate Authority's X.500d distinguished names are::

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

In order to give the certificate subject name of the certificate used by the Certificate Authority a distinguished name, the Certificate Authority

adopts the X.500 distinguished name format for subscribers:

C=TW, CN=Chinese name stored in the system database of the Department of Household Registration, or Chinese or English name stored the Entry, Exit and Immigration Agency Business Management System of the Immigration Agency, and serialNumber=a unique serial number automatically assigned to the subscriber by the Certificate Authority.

3.1.6 Identification, Authentication, and Role of Trademark

N/A.

3.1.7 Naming Dispute Resolution Procedure

The Certification Authority allows same subscriber names, but a serial number or ID number is provided in the distinguished name of Section 3.1.4 for distinction to maintain the uniqueness of the subscriber name.

However, when an automatically assigned serial number is repeated, the Certificate Authority may manually assign the serial number to maintain the uniqueness of the serial number and resolve the naming dispute.

3.2 Initial Registration

3.2.1 Method of Proving Possession of Private Key

The token is promoted by a card management center trusted by the Certificate Authority, and the key pair is produced in the token itself, and the Registration Authority Counter sends the subscriber's public key to the Certificate Authority through a safe channel when issuing the certificate, so that when a subscriber applies for a certificate, the subscriber needs not to prove the possession of a private key.

3.2.2 Group Identity Authentication

N/A. The subject of the certificate issued by the Certificate Authority is a natural person, and thus not requiring a group identity authentication procedure.

3.2.2.1 Authentication of Domain Name Owner

The object of the certificate issued by the Certificate Authority is a natural person, and thus requiring no domain name possession authentication 之procedure.

3.2.3 Personal Identity Authentication

3.2.3.1Application at Counter by People from Our Country

After a certificate applicant from our country shows the official copy of his/her national identity card, the RAO of the Registration Authority Counter should check whether the national identity card is valid via the database of Household Registration Office, MOI, and check whether the person recorded by this national identity card is indeed the applicant to confirm the applicant's identity.

Please refer to Section 4.1.1 for the applicant's identity and qualification.

3.2.3.2 Non-resident Application at the Counter

After the non-resident applicant shows his/her resident permit, the RAO of the Registration Authority Counter should check whether the resident permit holder is still in the period of legal residence through the entry, exit and immigration agency business management system of the Immigration Agency, MOI, and check whether the person recorded by the resident permit is indeed the applicant, to confirm the applicant's identity.

Please refer to Section 4.1.1 for the applicant's identity and qualification.

3.2.3.3 Management of Various Online Certificates

The Certificate Authority has eight certificate management items for processing online certificate operations, and the identity authentication methods for these eight online certificate operations are specified as follows:

(1) Online Certificate Suspension

The subscriber may use the subscriber code selected by the Registration Authority Counter of Section 4.2 as the basis for the identity authentication.

(2) Urgent Certificate Suspension

The subscriber may transmit the identity related document via fax or online

transmission and use it as the basis for the identity authentication. The detailed identity related document is described in Section 4.9.15 .

(3) Online Reactivation Certificate

The subscriber may use the subscriber code selected by the Registration Authority Counter as described in Section 4.2 as the basis for the identity authentication.

(4) Online Application Extension Certificate

The certificate subscriber of our country may use the personal identity authentication procedure in accordance with Level 3 of the assurance level of the certificate policy of the Certificate Authority to submit personal data or other supporting data in order to complete the identity recognition and authentication of the certificate applicant or subscriber. The approved or trusted groups or personal identity recognition and authentication methods adopted by the Certificate Authority are published on the website by the Certificate Authority. Website: https://moica.nat.gov.tw/.

(5) Online Certificate Application Re-issuance

The certificate subscriber of our country may use the personal identity authentication procedure in accordance with Level 3 of the assurance level of the certificate policy of the Certificate Authority to submit personal data or other supporting data in order to complete the identity recognition and authentication of the certificate applicant or subscriber. The approved or trusted groups or personal identity recognition and authentication methods adopted by the Certificate Authority are published on the website by the Certificate Authority. Website: https://moica.nat.gov.tw/.

(6) Online Certificate Application

The certificate subscriber of our country may use the personal identity authentication procedure in accordance with Level 3 of the assurance level of the certificate policy of the Certificate Authority to submit personal data or other supporting data in order to complete the identity recognition and authentication of the certificate applicant or subscriber. The approved or trusted groups or personal identity recognition and authentication methods adopted by the Certificate Authority are published on the website by the Certificate Authority. Website: https://moica.nat.gov.tw/.

(7) Online Application Email Written in Certificate

The subscriber may use the current valid certificate supplemented with his/her national identity card number, VAT number, or resident permit number, birthdate, and other information processed with electronic signature as the basis for identity authentication.

(8) Online Subscriber Code Modification

The subscriber may use the current valid certificate supplemented with his/her national identity card number, VAT number, or resident permit number, birthdate, and other information processed with electronic signature as the basis for identity authentication.

3.2.4 Unverified Subscriber Information

Unverified subscriber information shall not be written into the certificate.

3.2.5 Confirmation of Responsibility

When applying for a certificate, subscribers shall file an application with an official ID card and a valid resident permit according to the regulation of "Personal Identity Identification" as specified in Section 3.2.3.

3.2.6 Interoperability Standard

Not stipulated.

3.2.7 Data Accuracy

This management center should take the following into account for the accuracy of evaluated data and the evaluation process:

1. Existence Time of Provided Data.
2. Update Frequency of Data Source.
3. Data Provider and Purpose of Data Collection.
4. Data Availability.
5. Data Public Accessibility Level.
6. Relative Difficulty of Forging or Changing Data.

3.3 Identification and Authentication of Re-key Request

3.3.1 Identification and Authentication of Routine Re-Key

The re-key of certificate refers to the issuance of a new certificate with the same characteristics and assurance level of the old certificate, and the

new certificate has a new different public key (corresponding to a new different private key) and a different serial number, and may also be designated with a different term of validity.

If the term of use of the subscriber's private key expires and it is necessary to change the key, an application should be filed to the Certificate Authority again, and the Registration Authority Counter will perform the identification and authentication of the subscriber who re-apply for the certificate in accordance with the regulation of Section 3.2

3.3.2 Identification and Authentication of Re-key for Certificate Revocation

If the subscriber's private key needs to be changed due to the certificate revocation, the subscriber should file a re-application of the certificate to the Certificate Authority. The Certificate, Registration Authority Counter will perform the identification and authentication of the subscriber who re-applies for the certificate in accordance with the regulation as specified in Section 3.2.3.

3.3.3 Re-Key for Certificate Renewal

Certificate renewal refers to the issuance of a new certificate having the same certificate subject name, key and related information of the old certificate, and the new certificate only extends the term of validity (notAfter) by a period of time, and assigns a new certificate serial number.

When a certificate subscriber of our country applies for a certificate renewal at the counter or by entrusting others to handle the renewal, the identity identification and authentication of the subscriber are the same as those specified in the regulation as specified in Section 3.2.3. If the certificate renewal is processed online, the identity identification and

authentication will be performed in accordance with the regulations as specified in Section 3.2.3.3.

The maximum allowable number, period, and eligibility of the subscriber's certificate renewal are described in Section 6.3.2.2.

3.4 Identification and Authentication of Certificate Revocation Application

In any of the following circumstances, the subscriber shall file a certificate revocation application to the Registration Authority Counter:

(1) It is confirmed that the private key has been compromised.

(2) There is a significant change of information in the certificate, which is sufficient to affect its trustworthiness. For example, the subscriber's name, national identity card number, VAT number, or resident permit number has changed.

(3) The use of certificate is no longer required.

(4) The certificate is damaged or stolen.

In any of the following circumstances, the Certificate Authority may revoke the original certificate of a subscriber of our country without prior consent of the subscriber, and will inform the subscriber about the reason of revocation and related matters after the revocation:

(1) It is confirmed that the content in the certificate is not true.

(2) It is confirmed that the subscriber's private key is fraudulently used, forged, or compromised.

(3) It is confirmed that the Certificate Authority's private key or

system is fraudulently used, forged or compromised, which is sufficient to affect the trustworthiness of the certificate.

(4) It is confirmed that the subscriber's certificate is issued without complying with the procedure regulated by this Statement.

(5) It is confirmed that the subscriber violates the regulation of this Statement or related laws.

(6) Notification by official document of the judicial authority.

(7) Death, or declared death of the Subscriber.

(8) The subscriber's loss of nationality of R.O.C.

(9) The subscriber changes name.

(10) The subscriber changes national identity card number or VAT number.

(11) The subscriber applies for a change of certificate content.

(12) The subscriber applies for a re-key.

(13) Under the declaration of guardianship

(14) The Certificate Authority's system is damaged (such as by fire, earthquake, and other disasters) and cannot be recovered.

In any of the following circumstances, the Certificate Authority may revoke the original certificate of a non-resident certificate subscriber without prior consent of the subscriber, and will inform the subscriber about the reason of revocation and other related matters after the revocation:

(1) It is confirmed that the content in the certificate is not true.

(2) It is confirmed that the subscriber's private key is fraudulently used, forged, or compromised.

(3) It is confirmed that the Certificate Authority's private key or system is fraudulently used, forged or compromised, which is sufficient to affect the trustworthiness of the certificate.

(4) It is confirmed that the subscriber's certificate is issued without complying with the procedure regulated by this Statement.

(5) It is confirmed that the subscriber violates the regulations of this Statement or related laws.

(6) Notification by official document of the judicial authority.

(7) Death, or declared death of the Subscriber.

(8) The subscriber recovers or obtains the nationality of R.O.C.

(9) The subscriber changes name.

(10) The subscriber changes resident permit number.

(11) The subscriber applies for a change of certificate content.

(12) The subscriber applies for a re-key.

(13) Under declaration of guardianship or expiration of residence period.

(14) The Certificate Authority's system is damaged (such as by fire, earthquake, and other disasters) and cannot be recovered.

(15) Other reasons for the Immigration Agency of MOI to cancel or revoke the subscriber's residence permit and cancel the subscriber's permission to stay.

3.5 Identification and Authentication of Certificate Suspension and Reactivation

(1) For a certificate subscriber of our country nationality applying for a certificate suspension at the counter, the subscriber shall provide an official copy of the national ID card. After receiving the certificate suspension application, the Registration Authority Counter will confirm the identity of the subscriber in accordance with the regulations of Section 3.2.3 of this Statement and use it as the basis for determining whether to agree to the certificate suspension. The subscriber can also fill in a power of attorney of the MOICA certificate agency and entrust others to handle the certificate suspension at the counter, and the identity authentication is the same as that described in Section 3.2.3.

The subscriber can connect to the repository to apply for the certificate suspension, but the subscriber needs to fill in the certificate IC card number or the identity recognition data and its relative subscriber code as the basis for the identity authentication. When the subscriber forgets the subscriber code, the subscriber can process the certificate suspension at the counter. After the RAO confirms the subscriber's identity, the RAO will file a deactivation certificate application to the Certificate Authority on behalf of the subscriber, and the subscriber can process a reset of the subscriber code at the same time.

If the subscriber loses the certificate and forgets the subscriber code, and cannot use any of the aforementioned procedures to process the certificate due to the limitation of time and space, the subscriber can use the urgent certificate suspension procedure to

process the certificate suspension, and the subscriber must apply for urgent certificate suspension via fax or online, and attach written data containing the authenticable identity such as an ID card, photocopies of the front and back of a resident permit or the triplicate form of a policy report, and an urgent contact number with a name, and the personal signature. After receiving the application form, the Certificate Authority will contact the applicant by telephone and ask related questions for identity authentication and use them as the basis to determine whether or not to agree granting the urgent certificate suspension. Please refer to Section 1.5.2 "Customer service contact information, and related detailed procedures and forms" published on https://moica.nat.gov.tw of this Statement for the fax number.

If the aforementioned examination for temporary suspension application is not passed, the Certificate Authority will reject the certificate suspension.

(2) If it is necessary to reactivate the certificate after certificate suspension, the subscriber will have to do so at the counter or via an online procedure.

When the certificate reactivation is applied at the counter, the applicant should provide the official copy of his/her national identity card. After receiving the application data, the Registration Authority Counter executes the identity authentication according to the regulation of Section 3.2.3 of this Statement and uses it as the basis to determine whether or not to agree granting the certificate reactivation. The subscriber can also fill in a power of attorney of the MOICA certificate agency and entrust others to handle the certificate suspension at the counter,

and the identity authentication is the same as that described in Section 3.2.3.

In the online application for the reactivation certificate, the subscriber can connect to the repository to apply for the reactivation of certificate and must fill in the certificate IC card number or the identity recognition data and its relative subscriber code for identity authentication, which is used as the basis to determine whether or not to agree granting the certificate reactivation.

If the aforementioned examination for temporary suspension application is not passed, the Certificate Authority will reject the certificate reactivation.

4 Certificate Life Cycle Operating Specification

4.1 Application of Certificate

The applicant should read the Subscriber Agreement first, and then applies for the certificate if the subscribe agrees the content of the Agreement.

The Subscriber Agreement will be recorded on the Certificate Authority's website (https://moica.nat.gov.tw/) and the certificate application form.

4.1.1 Certificate Applicant

The applicant should be over 18 years old, a citizen of our country or non-resident holding a resident permit, and without declaration of guardianship.

4.1.2 Registration Procedure and Responsibility

1. Before the issuance of certificate, the identity of the certificate applicant shall be confirmed.
2. The certificate applicant shall provide the identity recognition related documents.
3. The subscriber's responsibilities are as follows:
   (1) The subscriber shall follow the related regulation of this Statement and confirm the accuracy of the provided application data.
   (2) After the Certificate Authority approves the application and issues the certificate, the subscriber shall confirm the certificate information and receive the certificate in accordance with the regulations as specified in Section 4.3.
   (3) After the subscriber receives the certificate issued by the Certificate

Authority, it means that the accuracy of the content of the certificate information is confirmed, and the certificate can be used in accordance with the regulation as specified in Section 1.4.1. If the content of the certificate content information is wrong, the subscriber should proactively notify the Certificate Authority and apply for revocation.

(4) The subscriber shall keep and use the certificate properly.

(5) If it is necessary to suspend, reactivate, revoke or re-apply the certificate, the subscriber shall handle it in accordance with the regulations as specified in Sections 3.4 and 3.5. When there is a leakage or loss of private key data and the certification revocation must be required, the subscriber shall notify the Certificate Authority immediately. However, the subscriber shall still bear all the legal responsibility of using the certificate before the leakage or loss of data.

(6) The subscriber shall carefully select the safe computer environment and trustworthy application system. If the rights and interest of the relying party are damaged due to the factors of computer environment or application system, the subscriber shall take their own responsibility.

(7) If normal operations fail during the use of the certificate, the subscriber shall seek other ways immediately to complete the legal actions that should be done with others, and shall not use the abnormal operation of the Certificate Authority as a defendant reason against others. If a third party makes any claim or request to the Certificate Authority because of it, the subscriber and relying party shall be responsible for the liability of the damage to the Certificate Authority and shall compensate for damages, and the compensation is limited to direct damages to the Certificate Authority, but does not include indirect damages.

4.2 Certificate Application Procedure

1. Certificate Application at Counter

Except online application, the applicant shall apply at the counter for the application of an original card for the first time. The certificate applicant of our country shall provide the official copy of his/her national identity card or the non-residence certificate application shall submit personal data or other supporting data according to the procedure of the personal identity authentication of Level 3 of the assurance level of the certificate policy for the RAO to confirm whether the application is for the applicant. After receiving the certificate application information, the Registration Authority Counter will perform the identity authentication in accordance with the regulation of Section 3.2.3 of this Statement and use it as the basis to determine whether to agree accepting the certificate application.

2. Group Certificate Application

When the RAO visits each organization to accept certificate applications at counter (depending on the business requirements), the certificate applicant of our country shall fill in a certificate application, and provides the official copy of his/her national identity card for the RAO to confirm in person whether it is an application for the applicant, and then the RAO performs the identity authentication of the certificate application form with confirmed identity according to the regulation as specified in Section 3.2.3 of this Statement, and uses it as the basis to determine whether or not to agree accepting the certificate application.

3. Online Certificate Application

The certificate applicant performs the identity authentication

according to the regulation as specified in Section 3.2.3 and handles the online certificate application operation according to the process. Mobile MOICA certificates can only be applied by online certificate application .

The applicant should select his/her personal subscriber code provided for the RAO to input into the Registration Authority Counter system. The subscriber code is used for unlocking a locked token, and it is also used when the operation of the token is disabled (enabled) for the certificate processing operation.

The applicant may apply to write the e-mail into the certificate when needed, and the Certificate Authority needs to verify the e-mail to be written into the certificate in accordance with the regulation as specified in Section 3.2.3 to ensure the application unit possesses the legal right of the e-mail.

4.2.1 Execution of Identification and Authentication Functions

This management center handles the identification and authentication according to the regulation specified in Section 3.2.3 “Personal Identity Authentication”.

4.2.2 Approval or Rejection of Certificate Application

This management center can approve the certificate application after completing the examination of application data, and the identity identification and authentication operations.

This management center may reject the issuance of certificate in any of the following circumstances:

1. Without passing the “Personal Identity Authentication” requirements specified in Section 3.2.3.
2. The applicant has violates the Subscriber Agreement.
3. Other matters identified by this Management Center as reasons for refusing the certificate issuance. The Certificate Authority has the right to refuse issuing the certificate to any individual and shall not be liable for any damage

to the certificate applicant whose certificate issuance is refused.

4.2.3 Processing Time of Certificate Application

If the application data comply with the following related regulations, the Certificate Registration Authority Counter should complete the identity authentication and data examination procedure within three working days .

4.3 Certificate Issuance Procedure

4.3.1 The Management Center's Operation during Certificate Issuance

The certificate is issued according to the following procedure:

1. Certificate Issued at the Counter

   (1) After confirming the identity of the certificate applicant 之 identity, the RAO will input the data of the certificate application into the Registration Authority Counter system.

   (2) After confirming the correct input data, the RAO will add a digital signature to the certificate application data through the IC card.

   (3) The Registration Authority Counter system will upload the related certificate application data to the Registration Authority.

   (4) After checking the correct RAO signature, the Registration Authority will apply to the Certificate Authority for a certificate by complete certificate application information.

   (5) The Certificate Authority returns the issued certificate, and the Card Management Center will write the issued certificate

into the applicant's token.

2. Online Certificate Issuance

   (1) After the identity of the certificate applicant is confirmed online by the RAO at counter according to the regulation of Section 3.2.3, the subscriber's application data will be uploaded to the Registration Authority.

   (2) After the Registration Authority checks and confirms that the identity inputted by the applicant is correct, the complete certificate application information is used to apply to the Certificate Authority for certificate.

   (3) The issued certificate is returned from the Certificate Authority, and the Registration Authority writes the token into the issued certificate.

The applicant may apply to write the e-mail into the certificate when needed, and the Certificate Authority needs to verify the e-mail to be written into the certificate in accordance with the regulation as specified in Section 3.2.3 to ensure the application unit possesses the legal right of the e-mail.

4.3.2 Notice to Certificate Applicant by this Management Center

1. After the certificate is issued, the certificate applicant will be notified by e-mail first, and will be notified separately by mobile phone SMS. If neither one of the aforementioned two contact methods of the certificate applicant is not provided, the certificate applicant will have to inquire at the counter by himself.
2. The certificate applicant may check the progress of the certificate application on the Certificate Authority's website.

3. If it is not agreed to issue the certificate, the certificate applicant should be notified by email or telephone and clearly informed of the reasons of not agree to the issuance.

4.4 Procedure of Accepting Certificate

1. This management center provides a certificate subject name and a certificate subject alias to the certificate applicant for review.
2. After the certificate applicant confirms the correct content, browses the webpage, and clicks the certificate acceptance, this Management Center will issue the certificate immediately and publish the issuance on the repository.
3. If the certificate applicant finds that the content of the certificate is incorrect, the certificate applicant shall immediately notify this Management Center or Registration Authority.
4. If the certificate applicant has not completed the certificate acceptance within 90 days, the application will become invalid automatically and will not be announced separately.

4.4.1 Element of Accepting Certificate

After the certificate applicant confirms that the certificate subject name and the certificate subject alias are correct and accepts them, this Management Center will use it as the basis for certificate acceptance.

4.4.2 Certificate Publication of this Management Center

This management center will publish the issued certificate in the repository to complete the certificate announcement operation.

4.4.3 Notice of Certificate Issuance to Other Individuals by this Management Center

This management center publishes the issued certificate in the repository.

4.5 Usage of Key Pair and Certificate

4.5.1 Use of Subscriber’s Private Key and Certificate

1. When using the private key, the subscriber shall carefully select the computer environment and trustworthy application system to prevent the

private key from being stolen or misused by malicious software and hardware, leading to damage to rights.

2. The subscriber's key pair shall be produced according to the regulation of Section 6.1.1 "Key Pair Production", and the subscriber must have the right of controlling the private key.
3. The subscriber's private key shall not be used for certificate issuance.
4. The subscriber shall protect the private key from being used or disclosed by other unauthorized persons, and ensure that the private key is used according to the key usage noted in the certificate extension field.
5. The subscriber must use the certificate according to the regulations of the certificate policy and this Statement.

4.5.2 Relying Party's Use of Public Key and Certificate

1. Before using the certificate issued by the Certificate Authority, the relying party shall confirm whether the type of certificate, , assurance level and key usage meets the application requirement.
2. The relying party shall process the critical and non-critical certificate extension field in accordance with the X.509 specification.
3. Before using the authentication service provided by the Certificate Authority, the relying party must carefully read this Statement, follow the regulations of this Statement, and pay attention to the amendment to this Statement.
4. The relying party needs to verify the validity of the certificates including the certificate and the certificate chain of all Certificate Authority's certificates.
5. The relying party shall check the certificate policy of the Certificate Authority and subscriber certificates to confirm the assurance level of the certificate.
6. The relying party shall confirm the certificate usage.

4.6 Certificate Renewal

Certificate renewal refers to the issuance of one new certificate having the same certificate subject name, key and related information of the original certificate, and the new certificate just extends the term of validity (notAfter) for a period of time and assigns a new certificate serial number.

When a certificate subscriber of our country applies for a certificate renewal at the counter or by entrusting others to handle the renewal, the

identity identification and authentication of the subscriber are the same as those specified in the regulation as specified in Section 3.1. If the certificate renewal is processed online, the identity identification and authentication will be performed in accordance with the regulations as specified in Section 3.2.3.3.

The maximum allowable number, period, and eligibility of the subscriber's certificate renewal are described in Section 6.3.2.2.

4.6.1 Reasons for Certificate Renewal

When the principle term of use of the certificate key pair of the Certificate Authority as specified in Section 6.3.2.2 expires, the certificate subscriber of our country can decide and choose to re-key or renew the certificate.

4.6.2 Applicant of Certificate Renewal

Within three years starting from 60 days before the certificate expires, if the subscriber selects to change the key, then the subscriber will not be allowed to extend the original certificate. On the other hand, if the subscriber selects to renew the original certificate, then the subscriber will not be allowed to change the key.

If a subscriber obtains an extension of the certificate, and applies for a certificate revocation, then the Certificate Authority will revoke all of the subscriber's certificates according to the key pair according to the coexistence and abandonment principle.

4.6.3 Certificate renewal Procedure

After the principle term of use of the certificate key pair of the Certificate Authority as specified in Section 6.3.2.2 expires, the certificate subscriber of our country can decide and choose to re-key or renew the

certificate.

When the certificate subscriber of our country wants to apply for certificate extension, the original certificate duration will be used as reference, and the certificate renewal application method is as follows:

Within three years starting from 60 days before the certificate expires, and the certificate is not deactivate and revoked, the subscriber can use the certificate renewal software to process the online extension, or go to any certificate Registration Authority Counter to process the extension at counter, and the subscriber can also fill in a power of attorney of the MOICA certificate agency and entrust others to handle the certificate renewal at the counter, and the identity authentication is the same as that described in Section 3.2.3.3.

4.6.4 Notice of Issuance of Certificate extension to Subscribers

N/A.

4.6.5 Element of Accepting Certificate Extension

N/A.

4.6.6 Announcement of Certificate Extension of Certificate Authority

N/A.

4.6.7 Notice of Issuance of Certificate Extension to Other Individuals by this Management Center

N/A.

4.7 Re-key a Certificate

It refers to the production a set of public key and private key pair, and the original registration information is used to apply to the Certificate Authority for the certificate issuance.

4.7.1 Reasons of Re-keying Certificate

Re-keying a certificate refers to the issuance of a new certificate with the same characteristics and assurance level of the old certificate, and the new certificate can also be assigned with a different term of validity, in addition to the brand new different public key (corresponding to the new different private key) and a different serial number.

If the term of use (10 years) of the subscriber's private key expires and it is necessary to change the key, the subscriber shall re-apply for a certificate to the Certificate Authority, and the Registration Authority Counter will perform identification and authentication in accordance with the regulations of Section 3.1 to re-apply a certificate for the subscriber.

4.7.1.1 Reasons of Re-key this Management Center's Certificate

1. The term of use of the private key for executing and signing the usage of the certificate expires.
2. This management center's certificate is revoked.

4.7.1.2 Reasons of Re-key of Subscriber Certificate

1. The term of use of the subscriber's private key expires.
2. The subscriber's certificate is revoked.

4.7.2 Certificate Re-key Applicant

1. Re-key this Management Center's certificate.
   The authorized personnel of this Management Center submits an application to the General Management Center for a subordinate certificate authority's certificate.
2. Subscriber's certificate re-key

Authorized personnel of government organization (agency)

4.7.3 Certificate Re-keying Procedure

1. This management center should re-apply for a certificate according to the related regulations of the certification practice statement of the General

Management Center.

2. The subscriber should handle the re-key certificate according to the regulations as specified in Section 4.1 “Certificate Application” and Section 4.2 “Certificate Application Procedure”.

4.7.4 Issuance Notice of Subscriber’s Re-key Certificate

The issuance notice should be handled according to the regulation as specified in Section 4.3.2 “Notice to Certificate Applicant by this Management Center”.

4.7.5 Procedure of Accepting Re-key Certificate

1. This management center handles the acceptance of the re-key certificate according to the related regulations of the certification practice statement of the General Management Center.
2. The subscriber handles the acceptance of the re-key certificate according to the related regulations as specified in Section 4.4.1 “Element of Accepting Certificate.

4.7.6 Announcement of this Management Center’s Re-key Certificate

This management center announces the re-key certificate in the repository, or transmits the re-key certificate to the subscriber.

4.7.7 Notifying other Individual after the Re-key of this Management Center

This management center announces the re-key certificate on the repository.

4.8 Certificate Modification

4.8.1 Reasons for Certificate Modification

This management center does not provide the service for the subscriber to perform certificate modification.

4.8.2 Certificate Modification Applicant

N/A.

4.8.3 Certificate Modification Procedure

N/A.

4.8.4 Issuance Notice of Subscriber Certificate Modification

N/A.

4.8.5 Elements of Accepting Certificate Modification

N/A.

4.8.6 Announcement of Certificate Modification of this Management Center

N/A.

4.8.7 Notice of Certificate Issuance to other Individuals by this Management Center

N/A.

4.9 Certificate Suspension and Revocation

This management center provides all-year-round (7x24) certificate suspension service, but not all-year-round (7x24) certificate revocation service.

4.9.1 Reasons of Certificate Revocation

In any of the following circumstances, the subscriber shall submit a certificate revocation application to the Registration Authority Counter:

(1) It is confirmed that the private key is compromised.

(2) There is a significant change of information in the certificate, which is sufficient to affect its trustworthiness. For example, the subscriber's name, national identity card number, VAT number, or resident permit number has changed.

(3) The use of certificate is no longer required.

(4) The certificate is damaged or stolen.

In any of the following circumstances, the Certificate Authority may revoke the original certificate of a subscriber of our country without prior consent of the subscriber, and will inform the subscriber about the reason of revocation and related matters after the revocation:

(1) It is confirmed that the content in the certificate is not true.

(2) It is confirmed that the subscriber's private key is fraudulently used, forged, or compromised.

(3) It is confirmed that the Certificate Authority's private key or system is fraudulently used, forged or compromised, which is sufficient to affect the trustworthiness of the certificate.

(4) It is confirmed that the subscriber's certificate is issued without complying with the procedure regulated by this Statement.

(5) It is confirmed that the subscriber violates the regulation of this Statement or related laws.

(6) Notification by official document of the judicial authority.

(7) Death, or declared death of the Subscriber.

(8) The subscriber's loss of nationality of R.O.C.

(9) The subscriber changes name.

(10) The subscriber changes national identity card number or VAT number.

(11) The subscriber applies for a change of certificate content.

(12) The subscriber applies for a re-key.

(13) Under the declaration of guardianship

(14) The Certificate Authority's system is damaged (such as by fire, earthquake, and other disasters) and cannot be recovered.

In any of the following circumstances, the Certificate Authority may revoke the original certificate of a non-resident certificate subscriber without prior consent of the subscriber, and will inform the subscriber about the reason of revocation and other related matters after the revocation:

(1) It is confirmed that the content in the certificate is not true.

(2) It is confirmed that the subscriber's private key is fraudulently used, forged, or compromised.

(3) It is confirmed that the Certificate Authority's private key or system is fraudulently used, forged or compromised, which is sufficient to affect the trustworthiness of the certificate.

(4) It is confirmed that the subscriber's certificate is issued without complying with the procedure regulated by this Statement.

(5) It is confirmed that the subscriber violates the regulations of this Statement or related laws.

(6) Notification by official document of the judicial authority.

(7) Death, or declared death of the Subscriber.

(8) The subscriber recovers or obtains the nationality of R.O.C.

(9) The subscriber changes name.

(10) The subscriber changes resident permit number.

(11) The subscriber applies for a change of certificate content.

(12) The subscriber applies for a re-key.

(13) Under declaration of guardianship or expiration of residence period.

(14) The Certificate Authority's system is damaged (such as by fire, earthquake, and other disasters) and cannot be recovered

(15) Other reasons for the Immigration Agency of MOI to cancel or revoke the subscriber's residence permit and cancel the subscriber's permission to stay.

4.9.2 Certificate Revocation Applicant

The following five types of certificate revocation applicants are approved by the Certificate Authority:

(1) Subscriber of certificate revocation.

(2) Judicial authorities handling certificates according to official documents

(3) Immigration Agency of MOI .

(4) Household Registration Office.

(5) Certificate Registration Authority Counter.

4.9.3 Certificate Revocation Procedure

4.9.3.1 Certificate Revocation Method

The subscriber revocation certificate IC card must be processed at counter, and the revocation mobile MOICA certificate can be processed at

counter or online.

1. Processing at Counter

The subscriber shall provide the official copy of his/her national identity card or resident permit. After receiving the certificate application data, the Registration Authority Counter will perform the identity authentication according to the regulations as specified in Chapter 3 of this Statement and use it as the basis to determine whether or not to agree revoking the certificate. After the examination of the certificate revocation application is passed, the subscriber can connect to the repository for the query of the certificate revocation situation.

2. Processing Online

The subscriber must use the MOICA certificate IC card signature as the basis of identity recognition for the online revocation MOICA certificate.

If the judicial authority notifies the revocation of a specific certificate by official document, then the Certificate Authority will revoke the certificate after the confirmation of the official document.

If the Immigration Agency, MOI notifies the cancellation of the resident permit, then the Certificate Authority will revoke the certification after the content of the notification is confirmed.

The Certificate Authority will reject the application for revocation certificate, if the examination of the aforementioned revocation application is not passed.

4.9.3.2 Announcement and Notice

1. The revoked certificate shall be added into the certificate revocation list no later than the next update, and the information of the certificate status shall be announced in the repository, until the revoked certificate expires.

2. This management center may notify the application about the result of the certificate revocation application by e-mail, telephone, or official document.

4.9.3.3 Certificate Problem Response Mechanism

1. The problem finder can reflect a certificate problem through the e-mail given in Section 1.5.2 “Contact information”.
2. This management center provides all-year-round (7x24) services of receiving the report of a certificate problem and making responses to the problem.
3. This management center shall provide a preliminary investigation report to the subscriber and the problem finder within 24 hours after receiving the certificate problem,.
4. This management center shall discuss with the subscriber and the problem finder altogether and revoked the certificate, if needed, according to the evaluation of the following guideline and the selected certificate revocation date:

(1) The contents (such as the range, content, severity, level of importance and risk of harm) of the claimed problem.

(2) The consequence of the certificate revocation (having direct and indirect influence on the subscriber and the relying party).

(3) The number of certificate problems of the certificate or the subscriber.

(4) The unit or personnel proposing the certificate problem.

(5) Related legal provisions.

The processing time for this Management Center to accept a certificate problem report or receives a certificate revocation notice shall be handled according to the regulation as set forth in Section 4.9.5 “Processing term for this Management Center to handle certificate revocations”.

4.9.4 Grace period of certificate revocation application

N/A.

4.9.5 Processing term for this Management Center to handle

certificate revocation request

The Certificate Authority shall complete the certificate revocation processing procedure within one working day after the Registration Authority Counter accepts the certificate revocation application.

4.9.6 Requirements for a Relying Party to Check the Certificate Revocation

Before a relying party uses a certificate issued by this Management Center, the relying party should check the certificate revocation list or online certificate status protocol response message announced by this Management Center to confirm the validity and accuracy of the certificate chain of the certificate.

4.9.7 Issuance Frequency of Certificate Revocation List

1. The certificate revocation list should be issued at least once a day, and its validity period shall not exceed 36 hours.
2. Within 24 hours after completing the operation of certificate revocation, this Management Center shall reissue a certificate revocation list.

4.9.8 Maximum Delay Time of Certificate Revocation List Release

This management center will release the next certificate revocation list before the next update time recorded in the certificate revocation list.

4.9.9 Online Certificate Revocation/Status Check Services

1. This management center provides the services for the certificate inquiry and download, the inquiry of the certificate revocation list and online certificate status protocol.
2. This management center provides online certificate status protocol response messages specification by the online certificate status protocol responder (OCSP Responder) in compliance with RFC 6960 and RFC 5019 standards.
3. This management center uses the private key for signature to sign the certificate of the online certificate status protocol responder of the RSA 2048 /SHA-256.

4. The certificate of the online certificate status protocol responder must include the extension field “id-pkix-ocsp-nocheck” that complies with the RFC 6960 specification.

4.9.10 Regulations of Online Certificate Revocation Check

1. The relying party must check the validity of the certificate by the certificate revocation list or online certificate status protocol inquiry services.
2. The subscriber at lease can use the HTTP GETmethod to carry out the online certificate status protocol inquiry service.
3. The certificate status information is updated real-time.
4. For unissued certificates, the online certificate status protocol inquiry service shall not reply its status as “Good”.

4.9.11 Revocation Announcement in Other Forms

1. This management center supports the online certificate status protocol stapling (OCSP Stapling) according to the RFC 4366 specification.
2. If a subscriber uses the aforementioned protocol to inquire the certificate status, this Management Center should request the subscriber to activate the online certificate status protocol stapling through subscriber agreement, technical inspection, or other related methods.

4.9.12 Other Special Rules When the Key is Compromised

Not stipulated.

4.9.13 Reasons of Certificate Suspension

The subscriber many apply for temporary deactivation of the certificate in the following two circumstances:

(1) The token of the certificate key pair is missing or stolen.

(2) The subscriber believes that it is necessary to apply for the temporary deactivation of the certificate.

The Certificate Authority may execute the certificate suspension in the following circumstances, without requiring the prior consent from the

subscriber:

(1) Based on the official notice of the Judicial Authority.

4.9.14 Applicant of Certificate Suspension

The following two can be applicants of the certificate suspension:

(1) Subscriber of the certificate suspension.

(2) Person handling the certificate suspension according to the official document of the Judicial Authority.

4.9.15 Certificate Suspension Procedure

(1) When a certificate subscriber of our country processes the certificate suspension at the counter, the certificate subscriber shall provide the official copy of his/her ID card. After receiving the certificate suspension application, the Registration Authority Counter will confirm the subscriber identity according to the regulation as described in Section 3.2.3 of this Statement, and use it as the basis to determine whether or not to agree with the certificate suspension. The subscriber can also fill in a power of attorney of the MOICA certificate agency and entrust others to handle the certificate suspension at the counter, and the identity authentication is the same as that described in Section 3.2.3.3 . The subscriber can also connect to the repository to apply for the certificate suspension, but the subscriber needs to fill in the certificate IC card number or the identity recognition data and its relative subscriber code, or the MOICA certificate IC card signature as the basis for the identity authentication. When the subscriber forgets the subscriber code, the subscriber can process the certificate suspension at the counter. After the RAO

confirms the subscriber's identity, the RAO will file a deactivation certificate application to the Certificate Authority on behalf of the subscriber, and the subscriber can process a reset of the subscriber code at the same time

If the subscriber loses the certificate and forgets the subscriber code, and cannot use any of the aforementioned procedures to process the certificate due to the limitation of time and space, the subscriber can use the urgent certificate suspension procedure to process the certificate suspension, and the subscriber must apply for urgent certificate suspension via fax or online, and attach written data containing the authenticable identity such as an ID card, photocopies of the front and back of a resident permit or the triplicate form of a policy report, and an urgent contact number with a name, and the personal signature. After receiving the application form, the Certificate Authority will contact the applicant by telephone and ask related questions for identity authentication and use them as the basis to determine whether or not to agree granting the urgent certificate suspension. Please refer to Section 1.5.2 "Customer service contact information, and related detailed procedures and forms" published on https://moica.nat.gov.tw of this Statement for the fax number.

If the aforementioned examination for temporary suspension application is not passed, the Certificate Authority will reject the certificate suspension.

4.9.16 Limit of Certificate Suspension Period

From the time of accepting the certificate suspension application by the Registration Authority Counter, the Certificate Authority will complete

the procedure of handling the certificate suspension within one working day.

When applying for the certificate suspension, the subscriber needs not to declare the required deactivation period, and the maximum period of the certificate suspension set by the Certificate Authority is the time period from the application approval date to the expiration date of the certificate (5 or 8 years).

If the subscriber has completed processing the reactivation certificate during the certificate suspension period,, then the certificate will restore its validity.

4.9.17 Certificate Reactivation Procedure

If the subscriber needs to restore the use of the certificate after the certificate suspension, the subscriber can complete the following procedure at counter or online.

When the certificate reactivation is applied at the counter, the applicant should provide the official copy of his/her national identity card. After receiving the application data, the Registration Authority Counter executes the identity authentication according to the regulation of Section 3.2.3 of this Statement and uses it as the basis to determine whether or not to agree the certificate reactivation. The subscriber can also fill in a power of attorney of the MOICA certificate agency and entrust others to handle the certificate suspension at the counter, and the identity authentication is the same as that described in Section 3.2.3.

In the online application for the reactivation certificate, the subscriber can connect to the repository to apply for the reactivation of certificate and must fill in the certificate IC card number or the identity recognition data and its relative subscriber code, or the MOICA certificate IC card signature for identity authentication, which is used as the basis to determine whether

or not to agree granting the certificate reactivation.

If the aforementioned examination for the reactivation certificate application is not passed, the Certificate Authority will reject the certificate reactivation.

4.10 Certificate Status Service

4.10.1 Characteristics of Service

The certificate revocation information in the certificate revocation list or online certificate status protocol response message is deleted only after the revoked certificate has expired.

4.10.2 Availability of Service

1. This management center provides all-year-round (7 x 24) uninterrupted repository service and certificate status inquiry service with a response time within 10 seconds.
2. If the repository service cannot work properly, the normal operation of the service must be recovered within two working days.
3. This management center provides all-year-round (7 x 24) response counter to handle high priority certificate problems. Please refer to Section 1.5.2 for contact information.

4.10.3 Optional Function

Not stipulated.

4.11 Termination of Service

If the certificate subscriber no longer uses the service of this Management Center, this Management Center agrees to the subscriber's termination of service under the following conditions:

1. The certificate expires.
2. The Subscriber revokes the certificate.

4.12 Private Key Escrow and Recovery

4.12.1 Policy and Practice of Key Escrow and Recovery

1. The private key used as the signature of this Management Center cannot be escrowed.
2. This management center does not provide the escrow or recovery of the subscriber's private key.

4.12.2 Policy and Practice of Key Packaging and Recovery for Communication

This management center does not provide key packaging and recovery for communication.

5 Infrastructure, Security Management and Procedural Control

5.1 Physical Control

5.1.1 Physical Location and Structure

The computer room of the Certificate Authority is located at the data center of the Ministry and in compliance with the government credibility and the computer room facility standard for storing high-importance and sensitive data, and it has access control, security, surveillance video, and other physical security mechanisms to prevent unauthorized access to the related equipment of the Certificate Authority.

5.1.2 Physical Access

The Certificate Authority operates at the third assurance level of physical control, and the computer room has four layers of access control. The first layer is the security guard on duty throughout the year, the second layer is the floor access control system, the third-layer is the computer room access confirmation control of other personnel by the personnel of the computer room, and the fourth layer is the chassis access control, wherein the chassis door can only be opened by the monitoring system operated by the computer room's physical management personnel.

Besides the access control system capable of restricting unauthorized personnel to approach the computer room, the chassis monitoring system can control the opening of the chassis to prevent unauthorized access of hardware, software, hardware cryptographic module , and related equipment.

Any portable storage media brought into the computer room must be

checked for confirmation of being free of no computer virus or any malicious software that may harm the system of the Certificate Authority.

People other than Certificate Authority's personnel entering and exiting the computer room shall fill in the entry and exit record and accompanied by related Certificate Authority personnel throughout the whole journey.

When a Certificate Authority related personnel leaves the computer room, the related personnel should carry out and record the following inspection to prevent unauthorized personnel from entering the computer room:

(1) Confirm whether the equipment is operating normally.

(2) Confirm whether the chassis door is shut.

(3) Confirm whether the access control system is operating normally.

5.1.3 Electricity and Air Conditioning

The Certificate Authority's computer room is equipped with an independent constant temperature and humidity air conditioning system to control the temperature and humidity of the environment, so that the computer room can maintain the best operating environment.

5.1.4 Flood Prevention and Protection

The Certificate Authority's computer room built at the 3rd floor or above of a building above the foundation, and there are waterproof facilities and pumps in the partition of building.

5.1.5 Fire Prevention and Protection

The Certificate Authority's computer room has an automatic fire detection function, and the system can automatically start the fire extinguishing equipment and has manual switches at the main entrances and exits of each computer room for the personnel at site to start the operation of the fire extinguishing equipment manually in emergency.

5.1.6 Media Storage

The storage media of audit log, archive, and backup data are stored in the Certificate Authority's computer room for one year, and then will be moved to a remote backup place for storage afterward.

5.1.7 Replaced Equipment Treatment

The Certificate Authority's important information, document and data as described in Section 9.3.1, when not needed, shall be shredded by a shredder. Before the magnetic tape, hard disk, floppy disk, magneto-optical disk (MO) or memory of another form is scrapped, the stored data shall be cleared by a format procedure, and the optical disk shall be physically destroyed.

5.1.8 Remote Backup

The distance between the remote backup computer room and the Certificate Authority is over 30 Km, which is long enough to avoid damaging both places at the same time when a disaster occurs. The backup content includes data and system programs, and the backup of all data should be carried out at least once a week, and the backup of changed data shall be carried out on the same day. The remote backup system and the Certificate Authority system have the same security level.

5.2 Procedural control

The Certificate Authority executes each trusted role of the related system operation by a procedural control and sets the number of personnel required for each job, and the identification and authentication of each role according to the regulation to ensure the security of the system operation procedure.

5.2.1 Trusted Role

In order to provide an appropriate division for executing the responsibility of the related system operation to prevent a malicious use of the system by someone without being noticed, the Certificate Authority clearly stipulates the duty of the trusted role and its executable operation

for each system access operation.

The Certificate Authority has a total of five different types of trusted roles, respectively; Administrator, Officer, Auditor, Operator and Controller, and each type of trusted role carries out the personnel control in accordance with the regulation as specified in Section 5.3 in order to prevent possible internal attacks. One type of trusted role can be held by a multiple of people, and each type of trusted role has a chief (or Chief Role). The job definition of the five types of trusted roles is explained as follows:

1. Administrator is responsible for:
   (1) Installing, configuring and maintaining the Certificate Authority system.
   (2) Creating and maintaining subscriber accounts of the Certificate Authority system.
   (3) Setting audit parameters.
   (4) Producing and backing up the keys of the Certificate Authority.
2. Officer is responsible for:
   (1) Starting or stopping the certificate issuance service.
   (2) Starting or stopping the certificate revocation service.
3. Auditor is responsible for:
   (1) Checking, maintaining and archiving the audit log.
   (2) Executing or monitoring internal audit to confirm whether the operation of the Certificate Authority complies with the regulation of this Statement.
4. Operator is responsible for:

   (1) Maintaining the daily operation of the system equipment.
   (2) Carrying out the system backup and recovery operations.
   (3) Updating the storage media.
   (4) Updating the software and hardware other than the Certificate Authority's certificate management system.
   (5) Maintaining the network and website: Establish system security and virus protection mechanism and network security event detection and notification, etc.

5. Controller is responsible for:

   (1) The physical security control of the system (such as computer room

access control management, fire protection, flood protection, and air conditioning system, etc.)

5.2.2 Required Number of People for the Jobs

According to the operation security requirements of each type of trusted role, the required number of people is listed below:

(1) Administrator: At least three qualified personnel serve in this position.

(2) Officer: At least three qualified personnel serve in this position.

(3) Auditor: At least two qualified personnel serve in this position.

(4) Operator: At least two qualified personnel serve in this position.

(5) Controller: At least two qualified personnel serve in this position.

The number of people for each task is listed below:

Task name	Administrator	Officer	Auditor	Operator	Controller
Installation, configuration and maintenance of the Certificate Authority certificate management system	2				1
Establishment and maintenance of subscriber accounts of Certificate Authority certificate management system	2				1
Setup of audit parameters	2				1
Production and backup of the keys of Certificate Authority	2		1		1
Start or stop of certificate issuance service		2			1
Start or stop of certificate revocation service		2			1
Inspection, maintenance and archive of audit log			1		1
Daily operation maintenance of system equipment				1	1
System backup and recovery operations				1	1
Update of storage media				1	1

Task name	Administrator	Officer	Auditor	Operator	Controller
Updates of software and hardware other than the Certificate Authority certificate management system				1	1
Maintenance of network and website				1	1
Setup of physical security control of the system					2

5.2.3 Role Identification and Authentication

The Certificate Authority uses the subscriber account, password and the system account management function and IC card of the system to identify and authenticate different roles of administrator, officer, auditor and operator, and uses the authority setting function of the central access control system to identify and authenticate the controller.

5.2.4 Division of Responsibility of Different Roles

According to the five trusted roles defined according to Section 5.2.1, the role assignment of the Certificate Authority shall comply with the following rules:

1. The three trusted roles (administrator, officer and auditor) shall not serve each other concurrently, but can concurrently serve as an operator.
2. A controller shall not concurrently work the jobs of the other four roles.
3. Any one trusted role shall not be allowed to carry out the self-audit function.

5.3 Personnel Control

5.3.1 Background, Qualification, Experience and Security Requirements

1. Security Evaluation for Screening and Hiring Personnel

(1). Evaluation of Personality.
(2). Evaluation of Applicant’s experience.
(3). Evaluation of Academic, Professional Competence and Qualification.

(4). Confirmation of Personnel Identity.

(5). Evaluation of Personnel's Ethical Conduct.

2. Personnel Assessment Management

Before hiring a person, related personnel of the Certificate Authority should carry out a qualification check to confirm the qualification and working ability of the person. After being hired, the newly hired employee must take appropriate education and training, sign for the responsibilities in writing, and take a yearly qualification review. If failing the qualification review, the related personnel will be transferred from the current position and reassigned to a position matched with the personnel's qualification.

3. Personnel Hire & Fire and Promotion Management

If the hire and contract employment terms, conditions or agreement has changed, especially when the personnel leaves or the employment agreement is terminated, the personnel will be abided by the agreement of maintaining confidentiality.

4. Agreement on maintaining confidentiality

5. All related personnel of the Certificate Authority bear the responsibility of maintaining confidentiality, and sign the non-disclosure agreement, and shall not leak confidential information by oral, photocopying, borrowing, delivery, publication, or other methods.

5.3.2 Background Check Procedure

Before the personnel of the trusted role of the Certificate Authority as described in Section 5.2.1 is hired, a qualification check is conducted to conform whether the documents related to his/her identity and qualification are true.

5.3.3 Education and Training Requirements

The Education and Training Requirements of each trusted role are listed below:

Trusted role	Education and Training Requirement
Administrator	1. Security authentication mechanism of this Management Center. 2. Operating procedure for installing, configuring and maintaining the system of this Management Center. 3. Operating procedure for establishing and maintaining system subscriber accounts. 4. Operating procedure for setting audit parameter s. 5. Operating procedure of production and backup of this Management Center's key. 6. Disaster recovery and business sustainability procedure.
Officer	1. Security authentication mechanism of this Management Center. 2. Certificate issuance operating procedure. 3. Certificate revocation operating procedure. 4. Disaster recovery and business sustainability procedure.
Auditor	1. Security authentication mechanism of this Management Center. 2. Use and operating procedure of the audit system of this Management Center. 3. Procedure of checking maintaining and archiving the audit log. 4. Disaster recovery and business sustainability procedure.
Operator	1. System backup operating procedure. 2. Procedure of maintaining the daily operation of the system equipment. 3. Storage media update procedure. 4. Disaster recovery and business sustainability procedure.
Controller	1. Procedure of setting the physical access control authority. 2. Disaster recovery and business sustainability procedure.

5.3.4 Requirements and Frequency of Personnel Re-

education and Training

In a software and hardware upgrade of the Certificate Authority, a change of working procedure, a change of equipment or related regulations, personnel re-education and training are arranged, and the training conditions are recorded to ensure that the personnel understand the change of the related operation procedures and regulations.

5.3.5 Frequency and Sequence of Job Rotation

(1) An administrator can be transferred to the officer or auditor position only after serving the original position for at least one year.

(2) An officer can be transferred to the administrator or auditor position only after serving the original position for at least one year.

(3) An auditor can be transferred to the administrator or officer position only after serving the original position for at least one year.

(4) Only those who pass the related education and training and review can serves as an administrator, officer and auditor.

5.3.6 Punishment for Unauthorized Action

If a Certificate Authority related personnel violates the certificate policy and the procedures announced by this Statement or the Certificate Authority will receive appropriate management and punishment. For serious events that cause damages, the Certificate Authority will take legal action and hold the violator accountable.

5.3.7 Regulation of Hiring Personnel

The Certificate Authority hires a person according to the regulations of Section 5.3 “Personnel Security Requirements”.

5.3.8 Provided Document Data

The Certificate Authority provides this infrastructure certificate policy, technical specification, this Statement, system operating manual, electronic

signature act and related documents to the Certificate Authority's related personnel.

5.4 Audit Recording Procedure

1. All security related events are kept in the security audit log, and can be accessed immediately for auditing.
2. The security audit log can be generated automatically by the system or by paper record manually.

5.4.1 Types of Event Records

1. Security Audit
   - Change of important audit parameters.
   - Attempt of deleting or revising the audit log.
2. Identification and Authentication
   - Attempt of setting up a new role
   - Manager adjusts the maximum tolerable number of authentication attempts
   - System log-in failure
   - Account unlock
   - Change of Identity Recognition Mechanism of the System
3. When this Management Center produces a key (excluding the production of a single-use key).
4. Access of the private key of this Management Center
5. Addition, deletion and storage of the public key
6. Export of the private key other than the single-use key.
7. Application process of certificate registration, revocation and status change.
8. Change of security related configuration settings.
9. Addition, deletion, and revising the access authority of the account
10. Change of format profile of certificate
11. Change of format profile of certificate revocation list
12. Change of server settings of this Management Center
13. Security of physical access and place
14. Abnormal event

5.4.2 Record Processing Frequency

This management center reviews the audit log once a month, and tracks and

investigates major events.

5.4.3 Audit Log Retention Period

The audit log is retained for two months. When the retention period expires, the auditor removes the data, and this processing cannot be represented by other personnel.

5.4.4 Protection of Audit Log

1. Signature and encryption technology are used to retain the audit log, and a media storage that cannot be changed should be used.
2. The private key for signing an event record shall not be used for other usages.
3. The private key of the audit system should have security protection measures.
4. The audit log shall be kept in a safe place.

5.4.5 Audit Log Backup Procedure

1. The electronic audit log is backed up once a week.
2. The audit system automatically and periodically archives the audit log once a day, a week, and a month.

5.4.6 Audit Log Compiling System

The audit log compiling system is built in the system of this Management Center, and the audit procedure is enabled when the system of the management center starts.

If the automatic audit system does not work normally, and the system data are at a high risk status, this Management Center will suspend the certificate issuance service until the problem is solved.

5.4.7 Notice to the Person Who Causes the Event

The audit system does not need to inform the individual who caused the event, since the event has already been recorded by the system.

5.4.8 Vulnerability Evaluation

This management center performs a vulnerability evaluation of the operating system, physical facility, certificate management system, and network.

5.5 Record Archive Method

5.5.1 Types of Archive Records

1. This management center applies to the General Management Center for the certificate related data.
2. Certification practice statement.
3. Important agreements.
4. System or equipment configuration setting.
5. Revised or updated content of the system or configuration settings.
6. Certificate application data.
7. Revocation application data.
8. Accepted confirmation records of the certificate.
9. Token activation record.
10. Issued or published certificate.
11. Record of re-keys of this Management Center.
12. Issued or published certificate revocation list.
13. Audit log.
14. Other instruction data or application for proving and supporting the archive content.
15. Documents required by audit personnel.
16. The organization identity authentication data are specified according to the regulation as specified in Section 3.2.2 “Authentication of Organization Identity”.

5.5.2 Archive Record Retention Period

1. Archived records and applications for the archive records are kept for a retention period of ten years.
2. After an archived record exceeds its retention period, any written data shall be destroyed in a safe manner, and the data files in can be backed up into other storage media with appropriate protections, or destroyed in a safe manner.

5.5.3 Protection of Archive Record

1. Adding, revising or deleting an archived record is not allowed.
2. The archived record should be transferred to another storage medium with a protection level not lower than the original protection level.

3. The archived record should be kept in a safe place.

5.5.4 Archive Record Backup Procedure

The archived record is backed up to the remote backup center.

5.5.5 Timestamp Requirement of Archive Record

1. The content of the electronic archived record should include date and time information which is protected by appropriate digital signature in order to check whether date and time information in the record has been changed without authorization.
2. The date and time information in the electronic record are the date and time of the computer operating system instead of the electronic timestamp data provided by a third party.
3. All computer systems of this Management Center conduct time adjustment regularly.
4. The written record of archive also records the date information, and the time information when needed. If there is a change of the recorded date and time, it shall be confirmed by the auditor's signature.

5.5.6 Archive Record Compiling System

This management center does not have an archive record compiling system.

5.5.7 Procedure of Obtaining and Verifying Archived Record

1. The archived record can only be obtained by written application with approval.
2. Auditor is responsible for verifying the archived record. For written documents, the authentication of the signer and date of the document must be verified. For electronic files, the authentication of the digital signature of the archived record must be verified.

5.6 Re-key

1. Before the term of use of an issued certificate expires, the private key of this Management Center should be completed with the key pair change operation of the issued certificate, and the subordinate certificate authority certificate issued by the Government Certificate General Management Center should be obtained.

2. The subscriber's private key is changed periodically according to the regulation as specified in Section 6.3.2 "Term of use of public key and private key", and the subscriber's re-key and application for the certificate should be handled according to the regulations as specified in Section 4.2 "Certificate application procedure".

5.7 Recovery Procedure When Key is Compromised or During Disaster

5.7.1 Procedure for Handling Emergency and Compromised System

This management center sets a procedure to report and handle emergency and compromised systems, and a drill is conducted yearly according to the procedure.

5.7.2 Procedure for Recovering Damaged Computer Resource, Software or Data

This management center sets a procedure for recovering damaged computer resource, software or data, and a drill is conducted yearly according to the procedure.

When any computer equipment is damaged and unable to operate, priority shall be given to the operation of recovering the repository and rebuild the certificate issuance and management capability immediately.

5.7.3 Procedure for Recovering Compromised Signature Key of this Management Center

This management center sets a procedure for recovering a compromised signature key, and a drill is conducted yearly according to the procedure.

5.7.4 Post-disaster Recovery of this Management Center's Security Facility

This management center conducts a drill yearly for the disaster recovery work of the security facility.

5.7.5 Procedure for Recovering this Management Center's

Signature Key of Revoked Certificate

This management center sets a procedure for recovering the signature key of a revoked certificate, and a drill is conducted yearly according to the procedure.

5.8 Termination of Service of this Management Center

1. Except for those who cannot be notified, the management center should notify all subscribers whose certificate is not revoked or expires, within 3 months before the scheduled termination of service, and make such announcement in the repository.
2. All valid certificates are revoked, and the custody and handover of file records are performed.

6 Technical Security Control

6.1 Production and Installation of Key Pair

6.1.1 Production of Key Pair

6.1.1.1 Production of this Management Center's Key Pair

The Certificate Authority produces the key pair in the hardware cryptographic module according to the regulation as specified in Section 6.2.1, and the production adopts the FIPS 140-2 security level random number generation mechanism and RSAkey algorithm. After the private key is produced in the hardware cryptographic module, the export and import of the key shall be handled according to the regulations as specified in Sections 6.2.2 and 6.2.6.

The production of the Certificate Authority's key pair s witnessed by the Electronic Certificate Promotion Committee members and related personnel, and conducted using a multi-person security control mechanism.

6.1.1.2 Production of Subscriber's Key Pair

The token used by the subscriber must comply with the specification as specified in Section 6.2.1, and its key pair is produced automatically in the token driven by the Certificate Authority's trusted card issuance center. After the production of the key pair is finished, its private key cannot be exported from the token.

The key pair of the mobile MOICA certificate is produced in the subscriber's trusted mobile device. After the production of the key pair is finished, its private key cannot be exported from the mobile device.

6.1.2 Private Key Safely Sent to Subscriber

After issuing the certificate, the Certificate Authority provides a private key to the subscriber and starts the token.

6.1.3 Public Key Safely Sent to this Management Center

The Registration Authority Counter sends the subscriber's public key to the Certificate Authority through a safe channel.

6.1.4 This Management Center's Public Key Safely sent to Relying Party

The Certificate Authority's own public key of a certificate is issued by the General Management Center, and announced in the General Management Center's repository, so that a relying party can directly download and use the public key. Before using the Certificate Authority's own public key, the relaying party shall use the public key according to the regulation specified by the General Management Center's certification practice statement. The relying party obtains the General Management Center's public key or a self-issued certificate through a safe channel, and then checks the signature of the Certificate Authority's public key certificate to the General Management Center to ensure that the public key in the public key certificate is reliable.

6.1.5 Key Length

The Certificate Authority uses the 2048-bit RSAkey and SHA256 hash function algorithm to issue the certificate, and the subscriber uses the RSA of 2048 bits or more, or the ECCkey of 521 bits or more.

6.1.6 Production and Quality Inspection of Key Parameter

1. The key parameter of the RSA algorithm is a null value.
2. The Certificate Authority adopts the ANSI X9.31 algorithm or the FIPS 186-3 specification to generate the prime numbers required for the RSA algorithm, so as to ensure that the primes are strong primes.
3. The subscriber's key generates the parameters required by the RSA or ECC algorithm in the token or the subscriber's mobile device according to the FIPS 186-3 specification.

6.1.7 Purposes of Use of Key

The Certificate Authority's own public key certificate is issued by the General Management Center, and key usage bits set for the certificate key

usage extension field are keyCertSign and cRLSign. The Certificate Authority's private key for signature is only used for the issuance of certificate and certificate revocation list.

The subscriber certificate includes two key pairs used for signature and encryption.

6.2 Private Key Protection and Cryptographic Module Security Control Measure

6.2.1 Standard and Control of Cryptographic Module

1. This Management Center uses the FIPS 140-2 security level 3 certified hardware cryptographic module to generate random numbers and key pairs.
2. IC cards or subscriber's trusted mobile device can be used as the storage media of the subscriber's key pair.
   (1) The IC card must pass the certification of the FIPS 140-2 security level 2 or equivalent level of safety.
   (2) The mobile device must pass the certification of the FIPS 140-2 security level 1 or equivalent level of safety.

6.2.2 Key Sharing Control

The multi-user control of the Certificate Authority's key sharing adopts the m-out-of-n secret sharing method (hereinafter referred to as m-out-of-n) provided by Shamir, and this method is a Secret Sharing method for Perfect Secrets and can be used for the backup and recovery of the private key sharing. This method has the highest degree of safety for the multi-user control of the Certificate Authority private's key, and thus it can also be used to activate the private key (Refer to Section 6.2.8).

6.2.3 Private Key Escrow

The private key used for the Certificate Authority's signature shall not be escrowed, and the Certificate Authority is not responsible for keeping the private key used for the subscriber's signature.

6.2.4 Private Key Backup

The private key backup uses high-security IC cards as the secret sharing storage media according to the regulation as specified in Section 6.2.2 “Multi-user control method of key sharing”.

6.2.5 Private Key Archive

The private key used for the Certificate Authority’s signature shall not be archived, and the Certificate Authority shall not archive the private key used for the subscriber’s signature.

6.2.6 Transmission between Private Key and Cryptographic Module

This Management Center performs the operation of inputting the private key into the cryptographic module in the following circumstances:

1. Recovery of key holding backup.
2. Change of the cryptographic module.

6.2.7 Private Key Stored in Cryptographic Module

The Certificate Authority can only enter the private key into the cryptographic module when it recovers the key backup or changes the cryptographic module. The private key should be entered into the cryptographic module in the multi-user control mode as specified in section 6.2.2. The method of inputting the private key can be of encryption or key sharing, to ensure that the key code will not be exposed to the cryptographic module during the input process. After the input of the private key is completed, all of the related important parameters of the production process must be destroyed.

6.2.8 Activation Method of Private Key

The Certificate Authority's private key is activated by the control of the m-out-of-n control IC cards, and the control IC cards for different usages are kept by the administrator and officer.

6.2.9 Deactivation Method of Private Key

The Certificate Authority's private key is deactivated by using manual multi-user authorization for the control.

6.2.10 Destruction Method of Private Key

In order to avoid the Certificate Authority's old private key from being stolen and affecting the accuracy of the issuance of the certificate, the Certificate Authority will complete a key update and issue a new certificate when the life cycle of the private key expires, and will no longer save the private key into the old private key stored in the hardware cryptographic module t after issuing the certificate or the certificate revocation list on the old private key, and will perform the zeroization of the content in the memory address, so as to destroy the old private key in the hardware cryptographic module. At the same time, the sharing of the old private key will also be physically destroyed.

6.2.11 Cryptographic Module Rating

The cryptographic module is rated according to the regulations as specified in Section 6.2.1 "Cryptographic Module Standard and Control" of the certificate policy.

6.3 Other Rules of Key Pair Management

The subscriber must manage the key pair by himself/herself, and the Certificate Authority is not responsible for keeping the subscriber's private

key for the subscriber.

The token of the key pair of the subscriber's certificate can be in different forms, but it has to comply with the specification as specified in Section 6.2.1, and the token includes two valid certificates used for signature and encryption.

However, if the subscriber chooses the re-key, the original certificate cannot be renewed within the period from 60 days before the expiration of the certificate to 3 years after the expiration. On the other hand, if the subscriber chooses to renew the original certificate, the subscriber cannot do the re- key

If the subscriber has obtained a renewed certificate and applied for a certificate revocation, the Certificate Authority will revoke all the subscriber's certificates based on the key pair co-existence and co-abolishment principle.

6.3.1 Archive of Public Key

The Certificate Authority will archive the certificate, and execute the security control of the archive system according to the regulation as specified in Section 5.5, and will not archive public key.

6.3.2 Term of Use of Public Key and Private Key

6.3.2.1 Term of Use of this Management Center's Public Key and Private Key

The key length of the Certificate Authority's public key and private key is RSA 2048 bits, and the term of use is at most 20 years, and the term of use of the private key for executing the issuance of the certificate is at most 10years, but it does not apply to the server certifications for issuing

the certificate revocation list and for the online certificate status inquiry (OCSP). However, if the certificate related application system is unable to modify the system in accordance with the re-key schedule, and the subscriber still needs to use the application system with the certificate issued by the old key. The period for the old key to execute the issuance of the certificate can be temporarily extended for convenience and better service.

6.3.2.2 Term of use of subscriber's public key and private key

The key length of the subscriber's public key and private key is RSA 2048 or more bits or ECC 521 or more bits, and the term of use of the public key certificate is 5 years, and the term of use of the private key is 5 years, and the term of use can be extended once for three years upon the expiration, and the term of use of the public key and the private key is at most 8 years.

The key length of the mobile MOICA certificate's public key and private key is RSA 2048 or more bits or ECC 521 or more bits, and the term of use of the public key certificate is 1 year, and the term of use of the private key is 1 year, and no extension or renewal is allowed upon expiration, and the production of a new key pair is required.

6.4 Protection of Activation Data

6.4.1 Generation of Activation Data

The Certificate Authority's activation data are generated by the hardware cryptographic module and then written into the m-out-of-n control IC cards. The activation data in the IC cards can be accessed directly by the built-in card reader of the hardware cryptographic module. The PIN code of the IC card can be inputted by the built-in keyboard of the

hardware cryptographic module.

6.4.2 Protection of Activation Data

The Certificate Authority's activation data is protected by the m-out-of-n control IC cards, and the PIN codes of the IC cards are kept by the custody personnel and shall not be recorded on any media. If the number of failed logins exceeds 3 times, the IC card will be locked; when the IC card is handed over, another custodial personnel must reset a new PIN code.

6.4.3 Regulations of Other Activation Data

The activation data of the Certificate Authority's private key shall not be archived.

6.5 Computer Software and Hardware Security Control Measure

6.5.1 Specific Computer Safety Technical Requirement

The Certificate Authority and its related auxiliary systems provide the following security control functions through the operating system, or the protective measures integrated with the operating system, software and physical hardware:

(1) Logon with identity authentication.

(2) Discretionary access control.

(3) Security audit ability.

(4) Access control limit for different certificate services and trusted roles.

(5) Trusted role and identity recognition and authentication.

(6) Password technology for ensuring the safety of each communication and database.

(7) Safe and reliable channel for trusted roles and related identity recognition.

(8) Procedure integrity and security control protection.

6.5.2 Computer Security Rating

The Certificate Authority's system and its operating environment comply with the security control principle of the WebTrust Principles and Criteria for Certification Authorities.

6.6 Technical Control Measure for Life Cycle

6.6.1 System Development Control Measure

The Certificate Authority adopts a dedicated physical or virtual host, and dedicated software and can only use components with security certification. The Certificate Authority does not install any hardware device or connect any network, device, or software is that are irrelevant to its operation. The Certificate Authority automatically checks whether there are malicious program codes every day.

6.6.2 Security Management Control Measure

For the first-time installation of the Certificate Authority's software, the Certificate Authority will confirm the correct version provided by the supplier and such version has not been revised. After the system installation, the Certificate Authority automatically checks the integrity of the software every day.

The Certificate Authority will record and control the configuration of the system, and any revision and upgrade, and will also detect any unauthorized revised system software or configuration.

6.6.3 Security Control Measure of Life Cycle

The current key is evaluated at least once yearly to check if there is any risk of system compromise.

6.7 Network Security Control Measure

The Certificate Authority's host and internal repository are installed in the demilarized zone (DMZ) of the external firewall through a dual firewall and an external network connection, and are connected to the Internet. Except the necessary maintenance or backup, uninterrupted certificate and certificate revocation list inquiry services are provided.

The Certificate Authority's internal repository information (including the certificate and the certificate revocation list) is protected by digital signature, and automatically transmitted from the internal repository to the external repository.

The Certificate Authority's external repository is protected by the updated system repair program, system vulnerability scan, intrusion detection system, firewall system and filtering router, etc. to prevent denial-of – service, intrusion, and other attacks.

The Certificate Authority should handle the related information security protection operation in line with the regulations as set forth in the information communication security management law.

6.8 Timestamp

In order to ensure the accuracy of the time below, the Certificate Authority

adjusts the system time according to the trusted time sources every hour.

1. Subscriber's certificate issuance time.
2. Subscriber's certificate revocation time.
3. Issue time of certificate revocation list.
4. Occurrence time of a system event.

6.9 Cryptographic module Security Control Measure

The cryptographic module security control measure is handled according to Section 6.1 "Production and installation of key pair" and Section 6.2 "Private key protection and cryptographic module security control measure".

7 Format Profile of Certificate, Certificate Revocation List and Online Certificate Status Protocol

7.1 Format Profile of Certificate

The format profile of the certificate issued by the Certificate Authority is in accordance with the related regulations as specified in the technical specification of this infrastructure.

7.1.1 Version of Serial Number

The Certificate Authority issues the X.509 v3 certificate in accordance with the RFC 5280 and ITU-T specifications.

7.1.2 Certificate Extension field

The extension field of the certificate issued by the Certificate Authority is in accordance with the related regulations as specified in the technical specification of this infrastructure.

7.1.3 Algorithm Object Identifier

The object identifier of the algorithm of the signature in the certificate issued by the Certificate Authority can be any one of the following:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256-with-RSA-Signature(11)}

(OID: 1.2.840.113549.1.1.11)

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384-with-RSA-Signature(12)}

(OID: 1.2.840.113549.1.1.12)

sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512-with-RSA-Signature(13)}

(OID: 1.2.840.113549.1.1.13)

The object identifier of the algorithm of the main public key in the certificate issued by the Certificate Authority is:

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

(OID: 1.2.840.113549.1.1.1)

7.1.4 Form of Naming

The X.500 distinguished name is used for the values filled in the two fields (main body and issuer certificate fields), and the attribute type of this name complies with the RFC 5280 related regulations.

7.1.5 Name Constraints

The certificate issued by the Certificate Authority does not use name constraints.

7.1.6 CPOID

The CPOID of this infrastructure is used.

7.1.7 Use of policy limit extension field

The certificate issued by the Certificate Authority does not use the policy limit extension field (policyConstraints).

7.1.8 Syntax and Semantics of Policy Qualifiers

The certificate issued by the Certificate Authority does not include policy qualifiers.

7.1.9 Semantic Process of Key Certificate Policy Extension field

The certificate policy extension field included in the certificate issued by the Certificate Authority must be marked as critical or not according to the provisions of government agency public key infrastructure Certificate

and the format profile of the certificate revocation list.

7.2 Certificate Revocation List Format Profile

7.2.1version serial number

The Certificate Authority issues the certificate revocation list (X.509 v2 version) in accordance with the RFC 5280 and ITU-T specifications.

7.2.2 Certificate Revocation List and Certificate Revocation List Entry Extension field

1. The certificate revocation list extension field (crlExtensions) and the certificate revocation list entry extension field (crlEntryExtensions) of the certificate revocation list comply with the related provisions of ITU-T X.509, RFC 5280, and format profile of this infrastructure certificate and certificate revocation list.
2. The necessary certificate revocation list extension field and certificate revocation list entry extension field and their keys used in the certificate revocation list are described in the “Format Profile of Government Agency Public Key Infrastructure Certificate and Certificate Revocation List”.
3. If other optional extension field is added in the future, the usage method shall comply with the regulations of the aforementioned standard.

7.3online certificate status protocol format profile

1. This Management Center provides an online certificate status protocol inquiry service in compliance with the RFC 6960 and RFC 5019 standards, and the website of this Management Center online certificate status protocol inquiry service is indicated in the certificate authority access information extension field of the certificate.
2. The online certificate status protocol query packet of this Management Center’s online certificate status protocol inquiry service should include the following information:

Version serial number

Target certificate identifier: including the hash function algorithm, certificate the hash value of the issuer’s name, the hash value of the certificate issuer’s public key, and the certificate serial number of the target certificate.

This Management Center online certificate status protocol response message includes

the following basic fields:

Field	Description
Version	v.1 (0x0)
Responder ID	The subject name of an online certificate status protocol responder
Produced Time	Time of signing the response message
Certificate Identifier to be Queried	Including hash algorithm, hash value of certificate issuer's name, hash value of certificate issuer's public key and serial number of the certificate to be queried
Certificate Status	Certificate status codes are given below: 0: stands for a valid certificate status. 1: stands for the status that the certificate has been revoked. If this field notes that the certificate has been revoked, it will be necessary to note the time and reason of this certificate revocation. The reason of revocation shall be the same as the reason code marked in the certificate authority revocation list. 2: stands for the unknown certificate status.
Duration (ThisUpdate/NextUpdate)	The suggested duration for responding messages includes this update time and the next update time
Signature Algorithm	The signature algorithm for responding messages can be sha256WithRSAEncryption
Signature	The signature of the responder of the online certificate status protocol
Certificate	The certificate of the responder of the online certificate status protocol

7.3.1 Version Serial Number

The version serial number is regulated according to the provisions of RFC 5019 and RFC 6960.

7.3.2 Online Certificate Status Protocol Extension field

1. The online certificate status protocol extension field complies with the regulations of Sections of RFC 5019 and RFC 6960.

2. The online certificate status protocol response message extension field shall include a certificate authority key identifier of the online certificate status protocol server.
3. If the online certificate status protocol query packet has a random number field, the online certificate status protocol response message shall also include the same random number field.

7.3.3 Operation Specification of Online Certificate Status Protocol Service

This management center's online certificate status protocol inquiry service is operated as follows:

1. This service can handle and receive the online certificate status protocol query packet transmitted by the HTTP GET/POST method to the online certificate status protocol subscribers.
2. The online certificate status protocol responder uses a short duration certificate, issued and updated by this Management Center periodically.

8 Audit method

8.1 Audit Frequency or Evaluation Matters

1. This management center executes an internal audit once a year.
2. This management center receives an external audit once a year, and the audit period shall not exceed 12 months.
3. The standard of the audit is WebTrust for CA.

8.2 Identity and Qualification of Audit Personnel

1. The auditing party shall be a qualified auditor authorized by a WebTrust for CA mark management unit to execute the WebTrust for CA and WebTrust for CA–SSL BR audit standard in our country.
2. The audit personnel shall be a qualified and authorized information system auditor or shall have the equivalent qualification.
3. During the audit, this Management Center should identify the identity of the audit personnel.

8.3 Relationship between Audit Personnel and Auditee

The audit personnel shall be independent of the auditee's Certificate Authority, and shall be an independent fair third party.

8.4 Scope of Audit

1. Whether or not this Statement complies with the regulation as specified in the certificate policy.
2. Whether or not this Management Center and Registration Authority operate according to this Statement.
3. This management center randomly samples at least 3% of the certificates (or samples one certificate if less than one certificate) each quarter for auditing.

8.5 Response Method to Audit Result

1. This management center improves the item that fails to meet the requirements and notifies the original audit personnel for review after making the improvement.

2. This management center may take necessary measures according to the type, severity and required correction time of the non-conformity.

8.6 Scope of Disclosing Audit Result

1. In addition to the risk of system security and the regulation as specified in section 9.3 “Business Information Confidentiality”, this Management Center shall publish the latest external audit report and management statement in the repository within three months after the end of the audit. For any postponed publication, an explanation letter signed by a qualified auditor shall be provided.
2. The audit result is shown on the home page of this Management Center’s website with the WebTrust Principles and Criteria for Certification Authorities mark and the external audit report and management statement can be read after clicking the mark.
3. The content of published audit document shall meet the related requirements of each browser’s trusted root certificate plan.

9 Other Business and Legal Matters

9.1 Fees

No charge for the time being.

9.1.1 Certificate Issuance, and Extension Fees

No charge for the time being.

9.1.2 Certificate Query Fee

No charge for the time being.

9.1.3 Certificate Revocation and Status Query Fee

No charge for the time being.

9.1.4 Other Service Fees

No charge for the time being.

9.1.5 Refund procedure

N/A.

9.2 Financial Responsibility

The operation of this Management Center is maintained by the government budgets without being insured by an insurance company. The financial responsibility is handled according to the government laws and regulations.

9.2.1 Insurance Coverage

N/A.

9.2.2 Other Asset

Not stipulated.

9.2.3 Insurance or Warranty Liability for End Entity

N/A.

9.3 Business Information Confidentiality

9.3.1 Scope of Important Information

1. The private key and passcode for the operation of this Management Center.
2. The related data of this Management Center's key sharing.
3. The subscriber data without consent of disclosure.
4. Records generated or kept by this Management Center and provided for auditing and tracking.
5. Audit logs and findings produced by an audit personnel during the auditing process, which shall not be fully disclosed.
6. Related business operation documents listed as non-disclosure documents by this Management Center.
7. Other data that shall not be disclosed by law.

9.3.2 Scope of General Information

Information other than those specified in Section 9.3.1 "Scope of Important Information" is basically general information.

9.3.3 Responsibility of Protecting Important information

This management center handles its important information according the regulations of the electronic signature act, WebTrust Principles and Criteria for Certification Authorities and personal data protection act, etc.

9.4 Privacy of Personal Information

9.4.1 Privacy Protection Plan

1. This management center publishes the privacy protection policy on its website.
2. This management center implements the privacy impact analysis, personal information risk assessment, and related measures.

9.4.2 Types of Confidential Data

1. Personal information recorded in a certificate application.
2. Personal information obtained by the operation of this Management Center.

9.4.3 Types of Non-confidential Data

The information other than those specified in Section 9.4.2 “Types of Confidential Data” are basically non-confidential data.

9.4.4 Responsibility of Protecting Confidential Data

The confidential data are protected according to the privacy protection policy published on the website, WebTrust Principles and Criteria for Certification Authorities, personal data protection act, and related regulations.

9.4.5 Announcement and Consent of Use of Private Information

1. The privacy protection policy is announcement on the website.
2. The use of personal private information must be agreed by the subscriber.

9.4.6 Release of Information by Judicial or Management Procedure

If the judicial authority or investigation unit needs to inquire important information due to investigation or collection of evidence, this Management Center will handle it by law without the need of notifying the subscriber.

9.4.7 Release of Other Information

The release is handled according to the related laws and regulations.

9.5 Intellectual Property Right

Except for personal data, the intellectual property right of the documents (including electronic files) produced by this Management Center belongs to this Management Center, and any reproduction or distribution of such documents shall be handled according to the copyright notice published on the website of this Management Center.

9.6 Responsibility and Obligation

9.6.1 Responsibility and Obligation of this Management Center

1. This Management Center runs its operation according to the requirements of Level 3 of the assurance level of the certificate policy and this Statement.
2. This Management Center executes the identification and authentication of the certificate application.
3. This Management Center issues, publishes, and revokes certificates.
4. This Management Center issues and releases certificate revocation lists.
5. This Management Center provides an online certificate status protocol inquiry service.
6. This Management Center produces and manages its private key.

9.6.2 Responsibility and Obligation of Registration Authority

1. This Management Center provides a certificate application service.
2. This Management Center executes the identification and authentication of the certificate application.
3. This Management Center manages the private key of the Registration Authority and shall not use the private key for any operation other than certificate registration.

9.6.3 Obligation of Subscribers

1. The subscriber should provide correct and complete information.
2. The subscriber should follow the related regulations of this Statement.
3. The subscriber should manage and use the private key properly.
4. If the private key is fraudulently used, compromised, or lost, this Management Center should be notified immediately to revoke the certificate, but the subscriber shall still bear all the legal responsibility of using the certificate before the abnormality.
5. The subscriber should safely produce his/her private key, and avoid the private key from being compromised.
6. The subscriber should carefully select a safe computer environment and a reliable application system. If the computer environment or the application

system itself causes damage to the rights of the relying party, the subscriber shall bear the responsibility.

7. If this Management Center fails to work normally for some reason, the subscriber should seek other ways as soon as possible to complete the legal actions that should be done with others, and this Management Center's abnormal operation shall not be used as a reason for defending against others.

9.6.4 Obligation of Relying Party

1. The relying party should comply with the related regulation of this Statement.
2. The relying party should carefully check the certificate digital signature, validity and key usage.
3. The relying party should ensure the safety of environment of using the certificate. For reasons not attributable to this Management Center, the relying party shall bear its own responsibility for any damage to the relying party.
4. If this Management Center fails to operate normally for some reason, the relying party should seek other ways as soon as possible to complete the legal actions that should be done with others, and must not use the abnormal operation of this Management Center as a reason to defend against others.

9.6.5 Obligation of Other Participants

This Management Center handles the outsourcing service according to the regulations as specified by the "Government Procurement Law" of MOI, and the contractor shall handle the outsourcing service according to the contract.

9.7 Disclaimer

If the subscriber or relying party fails to apply, manage and use the certificate according to the related regulations of this Statement, the damage to this Management Center caused by irresistible and other non-attributable reasons shall be the responsibility of the subscriber or relying party. The Management Center does not bear any legal responsibility.

9.8 Liability Limit

1. If it is necessary for this Management Center to suspend part of the certificate service due to system maintenance, conversion and expansion, or other reasons, announcement should be made in the repository 3 days before

suspending the service. The subscriber or relying party shall not use this as a reason for claiming damage compensation to this Management Center.

2. If the subscriber has a reason to revoke a certificate, the subscriber shall submit a certificate revocation application according to the regulations as specified in Section 4.9 “Certificate suspension and revocation”. After the approval of the certificate revocation application, this Management Center will complete the certificate revocation operation, issue a certificate revocation list and announce the certificate revocation in the repository within one working day.
3. Before the certificate revocation status is announced, the subscriber should take appropriate actions to reduce the impact on the relying party and bear all responsibilities caused by the use of the certificate

9.9 Compensation

9.9.1 Liability of this Management Center

If this Management Center fails to comply with this Statement and related laws and regulations and causes damage to the stakeholders' rights and interests, this Management Center shall be liable for liability; and the subscriber and relying party may request compensation in accordance with the related legal regulations.

9.9.2 Liability of Registration Authority

If the Registration Authority fails to comply with this Statement and related laws and regulations and causes damage to the stakeholders' rights and interests, the Registration Authority shall be liable for liability; and the subscriber and relying party may request compensation in accordance with the related legal regulations.

9.10 Term of Validity and Termination

9.10.1 Term of Validity

This Statement is approved by the General Management Center and will take effect after the announcement. The Statement will still be effective until it is replaced by a new version.

9.10.2 Termination

The termination of this Statement shall be resolved by the National Development Council, and approved by the General Management Center.

9.10.3 Validity of Termination and Existence

1. The description of the validity and termination of this Statement should be announced in this Management Center's repository.
2. After the termination of this Statement, the validity of this Statement should be maintained until the last issued certificate expires.

9.11 Individual Notice and Communication with Participant

Website announcement, repository, official document, letter, telephone, fax, and e-mail are used to establish the notice and communication channel between this Management Center, Registration Authority, subscriber and relying party.

9.12 Amendment

This Management Center yearly evaluates whether this Statement requires amendments, and implements the amendment after the approval by the General Management Center.

The amendment method is as follows:

1. Directly amend the content of this Statement.
2. Add or revise the content by attachments.

9.12.1 Amendment procedure

An amendment to this Statement will be announced after the review by the National Development Council and the approval by the General Management Center.

9.12.2 Notification Mechanism and Deadline

9.12.2.1 Notification Mechanism

All changes will be announced in the repository.

9.12.2.2 Change of Item

According to the different degree of influence of the changed item on the subscriber or relying party, the draft is announced in the repository after the review of the National Development Council. The notification period is as follows:

1. For large influences, the draft should be published in the repository for 15 days, before it is submitted to the General Management Center for review.
2. For small influences, the draft should be published in the repository for 7 days, before it is submitted to the General Management Center for review.

If this Statement needs to be typeset again, to change the vocabulary, or to correct a typographical mistake, announcement will not be made.

9.12.2.3 Opinion Response Deadline

When the subscriber or relying party has comments on the changed item, the response period is as follows:

1. For large influences, the response period is within 15 days from the announcement date.
2. For small influences, the response period is within 7 days from the announcement date.

9.12.2.4 Opinion Handling Mechanism

1. For those who have comments on the changes, please send the comments to this Management Center by e-mail before the deadline for reply.
2. After evaluation, this Management Center will reply and respond to the comments.

9.12.2.5 Publication Deadline

The amendment of this Statement is announced within 10 days in after the approval by the General Management Center.

9.12.3 Reasons for Amending CPOID

When the certificate policy is amended or its object identifier is changed, this Statement shall be in line with the amendment.

9.13 Dispute Processing Procedure

For the dispute between the subscriber and this Management Center, the two parties shall negotiate with the principle of good faith, and this Management Center

will provide explanation based on the related provisions of this Statement.

9.14 Governing Law

The governing law is based on e related laws and regulations of this country.

9.15 Applicable Law

The interpretation and legality of the related agreement signed by the Certificate Authority due to the need of executing the certificate issuance and management operations shall be handled in accordance with the electronic signature act and related laws and regulations.

9.16 Miscellaneous Clause

9.16.1 Entire Agreement

The agreement stipulated in this Statement constitutes the final and complete agreement between the main members. The main members include this Management Center, Registration Authority, subscriber and relying party. Even the main members have expressed the same matter verbally or written through other expressions, the agreement of this Statement shall ultimately prevail.

9.16.2 Assignment

The rights and obligations of a main member described in this Statement shall not be assigned to another party in any form without notifying this Management Center.

9.16.3 Severability

If any chapter of this Statement is not applicable and requires amendment, the other chapters will still be valid.

9.16.4 Contract Performance

If a subscriber or relying party of a certificate violates the provisions of this Statement and causes damage to this Management Center, and the damage is attributable to the subscriber's or relying party's intention or negligence, this Management Center may claim for damages, and claim and payment of the attorney

fees for handling the dispute or litigation from the attributable party.

9.16.5 Force Majeure

This management center affected by force majeure does not assume any legal responsibility for damages caused by irresistible and other non-attributable factors of this Management Center.

9.17 Other Clauses

Not stipulated.

Appendix 1: Glossary

◆ A

- **Activation Data**: Secret data, in addition to the key, required for accessing a cryptographic module (such as using the cryptographic module to open a private key for signature or decryption).
- **Applicant**: Subscriber, who applies to the Certificate Authority for a certificate but has not completed the certification procedure yet.
- **Archive**: Long-term data storage, physically separated from the main data storage), used for supporting the audit service, availability service, or integrity service, etc.
- **Assurance**: Basis for believing that the individual has complied with the specific security elements.
- **Assurance Level**: Certain level with a relative assurance level.
- **Audit**: Independent review and investigation to check whether the evaluation system control is proper in order to ensure the compliance with established policies and operating procedures, and suggest necessary improvements to the existing control, policy and procedure, etc.
- **Audit Log**: Records of system activities according to the time sequence of occurrence, which can be used to reconstruct or

investigate the sequence of events and the changes in a certain event.

- **Authenticate**: Procedure of verifying the legitimacy of a certain claimed identity, and verifying that such identity is belong to the person making the claim.

- **Authentication**

  - Procedure of establishing a subscriber or information system identity trust level.

  - Method used for establishing the security measures for data transmission, message, and source, or verifying the authority of receiving a specific type of information.

◆ **C**

- **Certificate**

  - Electronic proof containing signature verification data, used for confirming a signer's identity and qualification.

  - Digital presentation content of information includes:

    ✓ Issuing certificate authority.

    ✓ Subscriber's name or identity.

    ✓ Subscriber's public key.

    ✓ Valid term of certificate.

- ✓ Certificate Authority's digital signature.

- **Certificate Policy (CP)**: A management policy with a specific format established by the Electronic Exchange for the certificate management and execution. The certificate policy includes the related issues of generating, producing, transmitting, auditing, recovering (after being compromised) and managing the digital certificate. The certificate policy and its related technology can provide security services required by specific applications.

- **Certificate Problem Report**: Complaint of a key being compromised, a certificate being misused, or a certificate being forged, compromised, abused, or use improperly.

- **Certificate Revocation List (CRL)**

  - The Certificate Authority signs a revoked certificate list by digital signature, which can be used by a relying party.

  - A list maintained by the Certificate Authority, and recording the certificate issued by the Certificate Authority and revoked before expiry.

- **Certificate Authority (CA)**

  - An organization issuing certificates

  - An authority trusted by subscribers, and its business covering the issuance and management of the public key certificate in the X.509 format, the certificate authority revocation list, and

the certificate revocation list.

- **Certificate Authority Authorization (CAA)**: According to the provision of RFC 6844, the Certificate Authority Authorization DNS Resource Record allows the domain name owner of a domain name system to specify one or more certificate authorities to obtain authorization to help the domain to have an issued certificate, and announces the publicly trusted certificate authorities permitted and authorized by the Certificate Authority Authorization DNS Resource Record to implement additional controls, so as to reduce the risk of misrepresenting an unexpected certificate.

- **Certificate Modification**: It refers to providing a new certificate to the same certificate subject to replace the original certificate, but the expiration date of the new certificate must be the same as that of the old certificate, and the old certificate shall be revoked after the certificate modification.

- **Certification Practice Statement (CPS)**

  - It makes a public announcement and gives the guidelines for the Certificate Authority to issue certificates and process other verification services.

  - It states that a certain certificate authority's operation procedure of a certificate (including issuance, deactivation, revocation, extension and access, etc.) should meet specific requirements (as stated in the certificate policy or other service contract).

- **Certificate Transparency (CT)**: It is an open architecture for public monitoring and auditing of all certificates on the Internet (now TLS/SSL certificate is the priority target), through the issuance and existence of public certificates and provided for domain owners, certificate authorities, and domain subscribers to determine whether the certificate was issued by mistake or issued maliciously; in other words, its purpose is to provide a public monitoring and information disclosure environment that can be used to monitor the TLS/SSL certificate mechanism and review specific TLS/SSL certificates, so as to deter certificate related threats. The certificate is transparent, and the transparent mechanism is mainly composed of three elements: certificate transparency log, certificate monitor, and certificate audit.

- **Compromise**: Information is leaked to an unauthorized person or the information security policy is violated, resulting in unauthorized intentional or unintentional disclosure, modification, destruction or loss of information.

- **Cross-Certificate**: This is a certificate that establishes a trusted relationship between two root certificate authorities, and the cross-certificate is a certificate authority's certificate, but not a subscriber's certificate.

- **Cryptographic Module**: A set of hardware, software, firmware or a combination of the above, used for executing the logic or procedure of password (including password algorithm), and included within the password boundary of this module.

- **Cryptographically Secure Pseudorandom Number Generator, (CSPRNG)**: A random number generator used in an encryption system.

◆ **D**

- **Digital Signature**: An electronic document is computed into digital data of a certain length by a mathematical algorithm or other methods, encrypted with the private key pair of the signatory to form an electronic signature, which can be verified by a public key.

- **Certificate Duration**: A certificate field composed of two sub-fields: the start time of the term of validity and the end time of the term of validity.

◆ **E**

- **End Entity (EE)**: The following two types of individuals are includes in this infrastructure:

  - A private key owner responsible for keeping and applying the certificate.

  - A third party (who is not a private key owner or a certificate authority) who trusts the certificate issued by the Certificate Authority, that is the end entity is a subscriber and a relying party, including personnel, organizations, customers, devices, or stations.

- **ePKI Root Certificate Authority**: A root certificate authority of this infrastructure, which is the highest-level certificate authority in this hierarchical open architecture, and whose public key is the origin of trust.

◆ **F**

- **Federal Information Processing Standard (FIPS)**: An information processing standard cited by all government agencies and government contractors except military agencies established by U.S. Federal Government. Wherein, the cryptographic module security requirement standard is FIPS 140 standard (abbreviated as "FIPS 140"), and FIPS 140-2 divides the cryptographic module into 11 types of security requirements, and each security requirement category is divided into four security levels.

- **Fully Qualified Domain Name (FQDN)**: A definite domain name used for specifying the exact location of a computer in the domain hierarchy, and formed by a host name (a service name) and a domain name, and the host name must be place at the starting position of the name. Its example for reference is given below:

  - "ourserver.ourdomain.com.tw": "ourserver" is the host name, and "ourdomain.com.tw" is the domain name, wherein "ourdomain" is the third-level domain name, "com" is the second-level domain name, and "tw" is the country code top-level domain name.

  - "www.ourdomain.com": www is the host name, ourdomain is

the second-level domain name, and com is the universal top-level domain name.

◆ **I**

- **Information Technology Security Evaluation Criteria (ITSEC)**: It is the European security evaluation criteria proposed by the United Kingdom, France, Germany and other European countries in 1991 and defining seven security evaluation levels, respectively from E0 to E6. Unlike the reliable computer system security evaluation criteria, it only describes the requirement of the technology security, and uses confidentiality as a security enhancement function, while emphasizing the confidentiality integrity and availability of information security.

- **Internet Engineering Task Force (IETF)**: This task force is responsible for the development and promotion of the Internet standard, and its vision is to affect human design by means of producing high-quality technical documents, use and manage the Internet in order to make the operation of the Internet more smoothly. (Official website: https://www.ietf.org)

- **Issuing Certificate Authority (Issuing CA)**: In terms of a certificate, the certificate authority issuing the certificate is called the issuing certificate authority of the certificate.

◆ **K**

- **Key Escrow**: The subscriber must abide by the related

information as specified in the escrow agreement (or similar agreement) to store the subscriber's private key, and this escrow agreement requires one or more agencies. Based on the premise beneficial to the subscriber, the employer or the other party, the subscriber owns the subscriber's key according to the agreement.

- **Key Pair:** Two mathematically related keys with the following characteristics:
  - One of the keys is used for encrypting messages, and this encrypted message can be only decrypted by the other key.
  - It infeasible to derive one of the keys from the other key (from the perspective of computation).

◆ **M**

- **Mobile Device**
  - A mobile device refers to a portable device having basic computer functions and using a wireless communication interface to access network resources, which is also known as portable device.
- **Mobile MOICA Certificate**
  - Mobile MOICA certificate refers to the MOICA certificate installed and stored in a mobile identity recognition application of the Ministry of the Interior. The mobile identity recognition application of the Ministry of the Interior is installed in a

subscriber's reliable mobile device.

- **MOICA Certificate**
  - MOICA certificate refers to certificate issued according to this certification practice statement by the Ministry of the Interior Certificate Authority.

◆ **O**

- **Object Identifier (OID)**
  - A unique identifier which is composed of alphabets or numbers, and must be registered according to the registration standard established by international standard organizations, and can be used for identifying a distinguished corresponding certificate policy.
  - When a digital code in a special form is registered to the International Organization for Standardization mentions a certain object or a type of the object, this distinguished code can be quoted for identification. For example, in the public key infrastructure, this digital code specifies the certificate policy and the password algorithm so used.
- **Online Certificate Status Protocol (OCSP)**: An online certificate examination protocol, which allows a relying party to use software to determine the status of a certain certificate (such as a revoked certificate, a valid certificate, etc.)

- **Online Certificate Status Protocol Responder (OCSP Responder)**: An online service licensed and maintained by the Certificate Authority, which is connected to a repository for processing a certificate status inquiry request.

- **Online Certificate Status Protocol Stapling (OCSP Stapling)**

  - A TLS/SSL certificate status request extension field, capable of replacing the online certificate status protocol to become another method for checking the X.509 certificate status, and its operation mechanism is described below:

    ✓ The website obtains an online certificate status protocol response message with a "time limit' from the online certificate status protocol responder, and stores it temporarily.

    ✓ During the initial process of the TLS connection each time, the website will send this temporarily stored online certificate status protocol response message to a subscriber (generally a browser), and the subscriber only needs to verify the validity of the response message without requiring to send an online certificate status protocol query packet to the certificate authority.

  - This mechanism can forward the TLS/SSL certificate validity message periodically issued by the online certificate status protocol responder via the website, thus decreasing the frequency of checking the TLS/SSL certificate status from the

Certificate Authority by the subscribers and reducing the workload of the Certificate Authority.

- **Organization Validation (OV)**: In the SSL/TLS certificate issuance process, the identity of organization or personal subscribers is also identified and authenticated according to the assurance level of the certificate, besides the domain name control of the identified and authenticated subscribers, so that the connected and installed organization validation type SSL/TLS certificate website can provide a TLS encryption channel, know the owner of the website, and ensure the integrity of transmitted data.

◆ **P**

- **Private Key**: The key must be kept confidential in the following two cases.
  - A key used in the signature key pair for generating digital signature.
  - An encryption and decryption key used for decrypting the encrypted information.
- **Public Key**: The key shall be disclosed to the public in the following two cases (generally in the form of digital certificate).
  - A key used in the signature key pair for verifying the validity of digital signature.

- A key used in the encryption and decryption key pair for encrypting information.

- **Public Key Infrastructure (PKI):** A collection of law, policy, specification, personnel, equipment, facility, technology, process, audit and service, used for developing and managing asymmetrical cryptography and public key certificate on a broad scale.

◆ Q

- **Qualified Auditor**: An accounting firm, legal person or individual independent of the auditee, who meets the audit qualification requirements specified in Section 8.2 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the Certificate Authority and the browser forum.

◆ R

- **Registration Authority (RA)**

  - RA is responsible for confirming the identity or other attributes of the certificate applicant, but it does not issue certificates, nor does it manage certificates. Whether the Registration Authority is responsible for its action and the scope of responsibility shall be determined according to the applicable certificate policy or agreement.

  - RA is responsible for the identity identification and authentication of the subject of the certificate, but it does mot

issue certificates.

- **Re-key a Certificate**: It refers to the issuance of a new certificate with the same characteristics and assurance level of the old certificate, and the new certificate can also be assigned with a different term of validity, in addition to the brand new different public key (corresponding to the new different private key) and a different serial number.

- **Relying Party**

  - A party who trusts the digital signature of the received certificate and the public key contained in the useable certificate that can be verified, or the identity (or other attributes) of the naming subject contained in the trusted certificate and the corresponding relationship with the public key contained in the certificate.

  - An individual or organization receiving information containing the certificate and the digital signature, and may rely on these information (this digital signature can be verified by the public key listed on the certificate).

- **Renew a Certificate**: Issue a new certificate with the same certificate subject name, key, and related information of the old certificate in order to extend the term of validity of the certificate, and assign a new serial number to the renewed certificate.

- **Repository**

- A trustworthy system used for storing and searching a certificate or other certificate related information.
- Including certificate policy, certification practice statement, and certificate related information database.

- **Revoke a Certificate:** An operation of terminating a certificate before the valid duration of the certificate expires.
- **Root Certificate Authority (Root CA)**: A top-level certificate authority in the public key infrastructure, assigning an application software supplier to be responsible for distributing the self-signed certificate, in addition to the subordinate CA certificate and self-signed certificate. It can also be called the certificate General Management Center or the top-level certificate authority.

◆ **S**

- **Self-Signed Certificate:** It refers to a certificate whose issuer's name is the same as the name of the subject of the certificate. In other words, this certificate is issued by the private key having the same key pair for pairing with the public key and other information. It is a self-signed certificate in a public key infrastructure and can be used as a trustworthy origin of the certificate path, and its issuance object is the General Management Center itself, containing the public key of the General Management Center, and the name of the certificate issuer is the same as the name of the certificate subject, and can be used by a relying party to verify the digital signature of the General

Management Center's self-signed certificate, the Subordinate Certificate Authority's certificate, the cross-certificate and the Certificate Authority's revocation list.

- **Subordinate Certificate Authority**: In the hierarchical public key infrastructure, the certificate is issued by another certificate authority, and the activities of the subordinate certificate authority are limited by the certificate authority of such other certificate authority.

- **Subscriber**

  - A named or identified subject in the certificate, who holds the private key corresponding to the public key in the certificate.

  - An individual, including but not limited to a person, an organization, or a network device with the following properties:

    ✓ Subject stated on an issued certificate.

    ✓ Possessing a private key corresponding to the public key pair listed on the certificate.

    ✓ Does not issue certificate to other parties.

- **Secure Socket Layer (SSL)**: It is designed by Netscape, and mainly used for the secure communication protocol of the World Wide Web (WWW). It can encrypt network communication at the transport layer to ensure the data integrity of the transmission and can also verify the identity of the server and subscribers. Its

application is independent of the application layer protocol, so that before the application layer communicates, the encryption calculation, communication key negotiation, and server verification operation can be completed by this secure communication protocol. The latest version is SSL 3.0, whose design drawbacks were discovered by Google in October 2014, and recommended to be banned. At present, the TLS 1.3 version of the secure communication protocol is commonly used instead.

◆ T

- **Transport Layer Security (TLS)**: It is a safe communication protocol. In 1999, the Internet engineering task force standardized the SSL and announced the first version of TLS standard (RFC 2246), and then announced the updated versions of RFC 4346, RFC 5246 and RFC 6176, pointing out that the TLS 1.1 and TLS 1.2 versions and the latest versions are the RFC 8446 announced by the Internet Engineering Task Force in 2018 (which is the TLS 1.3 and has removed many outdated or insecure functions (including MD5 and SHA-224 encryption functions), and added support to ChaCha20, Poly1305, Ed25519, Ed448, x25519 and x448, while supporting 1-RTT and 0-RTT, to reduce the delay time of the connection between the server and the subscribers.

- **Trusted Computer System Evaluation Criteria (TCSEC)**: It is the first official standard for evaluating computer security, and was proposed by the U.S. Defense Science Board in 1970 and promulgated by the U.S. Department of Defense in 1985. It

divided the computer security into four levels and seven security levels, mainly focusing on the security of the operating system and does not emphasize on system integrity.

- **Trustworthy System:** This system includes computer hardware, software and procedure with the following properties:
  - Having a considerable protection function against invasion and misuse.
  - Providing reasonable availability, reliability and correct operation.
  - Executing predetermined functions appropriately.
  - Being consistent with the generally accepted security procedure.

Z

- **Zeroization**: Method of erasing the electronic stored data, and changing the data storage to prevent the data from being restored.

Appendix 2: Abbreviation of English Terms

Abbreviation	Full Name
AIA	Authority Info Access
CA	Certificate Authority
CAA	Certificate Authority Authorization
CP	Certificate Policy
CP OID	Certificate Policy Object Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DN	Distinguished Name
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments

Abbreviation	Full Name
SSL	Security Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security