Korea Information Certificate Authority

Certification Practice Statement

v.1.04

June 2019

Revision History

NO.	Version	Revision Date	Description
1.	V1.00	2018. 07. 23.	Certification Practice Statement Baseline Version Submitted
2.	V1.01	2018. 07. 30.	Certification Practice Statement details and related URL Updated
3.	V1.02	2018. 09. 04.	Certification Practice Statement Updated
4.	V1.03	2019. 04. 02.	AATL Object Identifier (OID) Submitted
5	V1.04	2019. 06. 19.	AATL Object Identifier (OID) Submitted

Table of Contents

1. INTRODUCTION

1.1. Overview

This document is prepared on the basis of RFC 3647 and establishes the matters necessary for the issuance, management and operation of certificates operated by Korea Information Certification (hereinafter referred to as the "Certification Authority" or “KICA”) and regulates the responsibilities and obligations of the parties concerned.

1.2 Document Name and Identification

This document is titled 'Certificate Practice Statement: CPS' and complies with the relevant laws of the Republic of Korea. The purpose of this document is to define matters concerning the work related to electronic signature certification, such as certification policies, certificate issuance and management, and operation policies of the Certification Authority, as well as matters concerning the responsibilities and rights of those involved in electronic signature certification systems.

The Policy Object Identifiers for AATL are subordinate to KICA Policy Object identifiers as shown below:

1.2.410.200085.2.1.1	– KICA Accredited Certificate
1.2.410.200085.3.1	– KICA AATL
1.2.410.200085.3.1.1.1.1	– KICA AATL – Individual Subscriber
1.2.410.200085.3.1.1.2.1	– KICA AATL – Individual Subscriber
1.2.410.200085.3.1.1.2.2	– KICA AATL – Individual Subscriber
1.2.410.200085.3.1.2.1.1	– KICA AATL – Organizational Subscriber
1.2.410.200085.3.1.2.2.1	– KICA AATL – Organizational Subscriber
1.2.410.200085.3.1.2.2.2	– KICA AATL – Organizational Subscriber
1.2.410.200085.3.2	– KICA Secure AATL
1.2.410.200085.3.2.1.1.1	– KICA Secure AATL – Individual Subscriber
1.2.410.200085.3.2.1.1.2	– KICA Secure AATL – Individual Subscriber
1.2.410.200085.3.2.2.1.1	– KICA Secure AATL – Organizational Subscriber
1.2.410.200085.3.2.2.1.2	– KICA Secure AATL – Organizational subscriber

1.3 PKI Participants

1.3.1 Certification Authorities

The Certification Authority provides the following certification services:

O Identification

O certificate issuance
O certificate revocation
O certificate related information announcement
O TSA (Time Stamping Authority) service
O OCSP (Online Certificate Status Protocol) Service

1.3.2 Registration Authorities

The Certification Authority may operate and manage the RA(Registration Authority) for outsourcing of work such as identification.

1.3.3 Subscribers

'Subscriber' means a person who has been issued a certificate from a Certification Authority, including individuals and businesses.

1.3.4 Relying Parties

Relying Parties mean the individuals and businesses who trust and use the certificate issued by the Certification Authority.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

A certificate issued by a Certification Authority is used to verify and prove that the certificate corresponds to the private key owned by the subscriber. A certificate issued by Certification Authority is a certificate for electronic signature, which is used to sign electronic documents (such as contract documents).

1.4.2 Prohibited Certificate Uses

The certificate shall only be used within the scope of use or purpose at the time of issuance. No one shall misuse the certificate beyond the scope or purpose of the certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Certification Authority as a certification service provider establishes and revises the CPS.

1.5.2 Contact Person

Contact information regarding the establishment and revision of the CPS is as follows.

O URL: trust.signgate.com
O E-mail: webmaster@signgate.com
O Address : 5th Fl, C-dong PDC, 242 Pangyo-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
O Phone : 02-360-3251

1.5.3 Person Determining CPS Suitability for the Policy

Certification Authority may amend the CPS when the Director of the Technical Research

Center determines that a change in CPS is necessary.

1.5.4 CPS Approval Procedures

The Certification Authority publishes the revised CPS on its website. The revised CPS will take effect on 10 days after posting on the website.

1.6 Definitions and Acronyms

O DN(Distinguished Name): means a form of name used to verify the issuer and owner of a certificate

O Electronic Message: means information, prepared, transmitted, received, or stored in an electronic form by an information processing system

O Digital Signature: means information that can verify the identity of a person who created the electronic messages and any changes to the electronic messages that is distinct to such electronic message

O Private Key: means a set of electronic information used to generate a digital signature

O Public Key: means a set of electronic information used to verify a digital signature

O Certification: means the act of ascertaining and verifying that the private key is held and known only by the subscriber

O Certificate: means a set of electronic information ascertaining and verifying that the private key is only held by and known only to the subscriber

O Certification Authority: means a trusted authority that issues digital signature certificates, regularly issues a certificate revocation list and certification works, such as publishing certificates and certificate revocation list on the directory system

O Registration Authority: means an authority that performs affairs that include verification of applicant identification, registration and management of subscriber information, application of certificates and application for revocation of certificates, among the certification works

O Object Identifier (OID): Certificates include algorithm, certificate policy, key usage, certificate properties, etc., in addition to the basic information such as DN(Distinguished Name), issuer, version, etc. An item to be represented by such information is called an object. In order to uniquely identify these objects, without repetition, a method of assigning identifiable number to each object is used and means an object identifier.

O Subscriber: means an individual or a business operator whose certificate has been issued by the Certification Authority

O Time Stamping Authority (TSA): A service system that proves that there was a legal proof at the time of creation of an electronic message and that it existed at a certain point in order to prevent illegal or unauthorized alteration.

O Online Certificate Status Protocol (OCSP): means an online certificate status protocol of a certificate that can verify the status of a certificate in real-time without obtaining a certificate revocation list

O Certification Work: means the affairs of managing the certificates and certification related records, etc., such as issuance, renewal and revocation of certificates, registration and changes of subscriber information, publication of certificate revocation list, etc.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Certification Authority shall post all application forms and related rules necessary for the certification services, including the CPS, on the website.

2.2 Publication of Certification Information

The Certification Authority shall post all information related to the issuance and management of a certificate, other than the personal information protected under the laws, on the website for anyone to verify such facts at any time.
O Certificate Practice Statement: trust.signgate.com
O Certificate Revocation List: ldap://signca.signgate.com:389
O Certificate of the Certification Authority: trust.signgate.com

2.3 Time or Frequency of Publication

The Certification Authority shall regularly post a certificate suspension and certificate revocation list on a daily basis. Amendments to the CPS shall be posted on the website 10 days prior to the effective date for anyone to verify.

2.4 Access Controls on Repositories

Information related to the CPS and issuance and management of certificates, etc. shall be posted on the website for anyone to verify such facts.
The Certification Authority shall protect the confidential information to be not disclosed nor changed. (Refer to Article 9.3)

3. IDENTIFICATION AND AUTHENTICATION OF CERTIFICATE

3.1 Certificate Naming and DN Structure

3.1.1 Types of Names

X.500 DN standard shall apply to the names used in the standard areas within the certificates and certificate suspension and certificate revocation list.

3.1.2 Meaning of Name

DN within the certificate issued by the Certification Authority shall use individual names, personal identification numbers, business names or business identification numbers.
For certificates of AATL digital signature usage, DN shall use individual names or business names.

3.1.3 Anonymous Certificate that cannot identify the applicant

The Certification Authority shall not issue anonymous certificates that cannot identify the applicants.

3.1.4 Rules for Certificate DN

X.500 and ASN.1 shall apply to the certificate DN issued by the Certification Authority.

3.1.5 Uniqueness of Certificate DN

DN of certificates shall have unique values.

3.1.6 Using Trademarks in Certificate DN

Certificate applicants shall be prohibited from using trademarks that infringe on the intellectual property rights of others.

3.2 Initial Identification

3.2.1 Method to Prove Possession of Private Key

The applicant or a representative of the applicant shall prove the possession of his/her private key by providing a Certificate Signing Request in the PKCS#10 format or cryptologically similar verification format.

3.2.2 Identification of a business

Certification authority or registration authority shall verify the identity of the licensee through one of the following three methods:

O business license number
O business license
O business email verification

3.2.3 Personal identification

Certification authority or registration authority shall verify the identity of the licensee through one of the following two methods:

O Personal identification number
O Identification service agency

3.2.4 Non-Verified Subscriber Information

A certificate shall not be issued for an application for a certificate that has not been identified.

3.2.5 Verify Permissions

The certification authority or registration authority shall identify the applicant's rights by the following methods.

O In case of an individual, one's identity is verified based on the criteria and methods of identification through one's identification number or the identification service agency.
O In case of a business operator, the identity of the licensee is verified by business license number, business registration card, or e-mail information.
O In case of a business representative, use business registration card, work certificate, or phone and e-mail information of the corporation to determine whether the registration agency has the right to delegate at a value that can identify the applicant.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Key Replacement Requests

3.3.1 Identification and Authentication for Routine Key Replacement

Not applicable.

3.3.2 Identification and Authentication for Key Replacement after Certificate Revocation

The Certification Authority and Registration Authority shall perform a verification procedure similar to the initial identification of Article 3.2 for a request of key replacement after the certificate revocation.

3.4 Identification for Certificate Revocation Request

A subscriber may revoke the certificate by verifying the identity with a valid certificate and password or personal identification number when a subscriber suspect that the certificate and key pair are no longer used or damaged. Identification and authentication on the revocation requests for the certificates used for AATL digital signature shall be verified through the use of a valid certificate and password.

4. CERTIFICATE MANAGEMENT PROCEDURES

4.1 Certificate Application

4.1.1 Certificate Applicant

A subscriber may apply for an issuance of a certificate through identification authentication, and the subscribers may be individuals or business operators.

4.1.2 Certificate Application Procedure and Responsibilities

A subscriber shall apply for an issuance of a certificate through on-line, after the identification authentication pursuant to a procedure stipulated in the CPS. The Certification Authority shall not generate nor retain a private key of a subscriber.

4.2 Certificate Application Processing

4.2.1 Identification and Authentication Procedure

The Certification Authority or the registration authority shall authenticate the identification according to the procedures stipulated in Article 3.2 of this CPS.

4.2.2 Approval or Rejection of Certificate Applications

The Certification Authority or the registration authority may reject the certificate application when not satisfying the procedures stipulated in Article 3.2 of this CPS.

4.2.3 Time to Process of Certificate Applications

When a subscriber’s identification authentication has been properly processed pursuant to Article 3.2 of this CPS, the Certification Authority shall issue the certificate within 7 days after the certificate request.

4.3 Certificate Issuance

4.3.1 Certificate Issuance Procedure

The Certificate Authority shall issue the certificate after verifying the following items through the issuance system prior to a new certificate issuance.
O Verification on the uniqueness of the public key information submitted by the subscriber
O Verification of the DN value and the usage of the key submitted by the subscriber

4.3.2 Certificate Issuance Notification

The Certification Authority shall notify the issuance of the certificate with an issuance message or via an e-mail address provided by the subscriber at the time of the application upon issuing the certificate.

4.4 Certificate Acceptance

4.4.1 Certificate Acceptance Procedure

A subscriber shall issue and accept the certificate through the certificate issuance management program. When the subscriber accepts the concerned certificate, the subscriber shall be deemed to have approve the accuracy of the information related to the issued certificate.

4.4.2 Certificate Acceptance Notification

The Certification Authority shall not post a certificate of a subscriber in a public storage. Provided, when the subscriber requests a certificate, it may be provided.

4.4.3 Publish Certificates to Trusted Parties

The Certification Authority shall not post a certificate of a subscriber to trusted parties.

4.5 Key Pair and Certificate Usage

4.5.1 Usage of Subscriber’s Private Key and Certificate

The private key of a subscriber shall be used only for performing the certification works, such as the digital signature and encrypted communications, etc.

4.5.2 Usage of Trusted Parties’ Public Key and Certificate

Not applicable.

4.6 Certificate Renewal

Certificate renewal shall not be acknowledged, as a policy. A subscriber whose certificate has expired shall be issued a new certificate, and such procedure shall be same as a new issuance.

4.6.1 Certificate Renewal Criteria

Not applicable.

4.6.2 Certificate Renewal Applicant

Not applicable.

4.6.3 Certificate Renewal Procedure

Not applicable.

4.7 Certificate Key Replacement

4.7.1 Certificate Key Replacement Criteria

The subscriber may receive certificate key replacement when applicable to any one of the following.
O When the subscriber forgets the certificate password
O When there is a concern for damages, leaks or changes to the private key of a subscriber

4.7.2 Certificate Key Replacement Applicant

Certificate key replacement may be performed by the Certification Authority or may be applied by the subscriber.

4.7.3 Certificate Key Replacement Procedure

Certificate key replacement shall be proceeded with the same procedure as a new issuance of a certificate.

4.7.4 Certificate Key Replacement Notification

Notification of certificate key replacement shall be proceeded with the same procedure as a new issuance of a certificate.

4.7.5 Certificate Key Replacement Acceptance

Approval of certificate key replacement shall be proceeded with the same procedure as a new issuance of a certificate.

4.7.6 Certificate Key Replacement Publication

Posting of certificate key replacement shall be proceeded with the same procedure as a new issuance of a certificate.

4.7.7 Certificate Key Replacement Notification

Notification of certificate key Replacement shall be proceeded with the same procedure as a new issuance of a certificate.

4.8 Certificate Modification

Certificate Authority shall not modify the contents of an issued certificate. It shall be processed by classifying into new certificate issuance or key replacement of a certificate according to the information requested by a subscriber.

4.8.1 Certificate Modification Criteria

Not applicable.

4.8.2 Certificate Modification Applicant

Not applicable.

4.8.3 Certificate Modification Procedure

Not applicable.

4.8.4 Certificate Modification Notification

Not applicable.

4.8.5 Certificate Modification Acceptance

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Reasons for Certificate Revocation

The Certification authority shall revoke the certificate of the subscriber in the event of any of the following reasons.

- O subscribers apply for certificate revocation
- O Subscriber has received or used the certificate in bad faith or other illegal manner or if the possibility is objectively recognized
- O If the subscriber's private key is found to be lost, corrupted, stolen or leaked
- O Subscribers violate this Certification Practice Statement.
- O subscriber has not applied for restoration within the deadline for applying for certificate revocation
- O If the Certificate Authority recognizes that the identity verification of the subscriber has not been legally performed

4.9.2 Certificate Revocation Applicant

A subscriber may apply for a certificate revocation. The Certification Authority may revoke a certificate of a subscriber pursuant to the grounds for revocation under Article 4.9.1.

4.9.3 Certificate Revocation Procedure

A subscriber may apply for a revocation of a certificate to Certification Authority after an identification authentication procedure conforming with the new issuance application. When Certification Authority becomes aware of an improper issuance of a certificate or becomes aware of loss or leak of a private key of a subscriber, the Certification Authority may revoke the certificate under its own authority, without a subscriber’s request.

4.9.4 Certificate Revocation Grace Period

The Certification Authority shall not have grace period for certificate revocation.

4.9.5 Certificate revocation period

The Certification Authority shall commence the certificate revocation within 24 hours after the application for revocation.

4.9.6 Verification requirements for certificate revocation for trusted parties

The Certification Authority provides a certificate revocation list to validate certificates.

4.9.7 CRL Issuance Frequency

The online certification revocation list shall be issued regularly, at least once a day, and the off-line certification revocation list shall be issued regularly, at least every 90 days.

4.9.8 Maximum Latency for CRLs

The online certification revocation list shall be issued within 1 day, at the latest, from the issuance date. The offline certification revocation list shall be issued within 10 days, at the latest, from the issuance date.

4.9.9 Online Certificate Status Protocol (OCSP)

The Certification Authority supports Online Certificate Status Protocol (OCSP) of subscriber certificates issued by KICA. Online certificate status verification (OCSP) addresses are as

follows:
O URL : http://signocsp.signgate.com:9020

4.9.10 OCSP Requirement

The verifier of a certificate shall verify the validity of a certificate by using an online certificate status protocol (OSCP).

4.9.11 Other Notification Methods of Certificate Revocation

Not applicable.

4.9.12 Special Requirements for Key Replacement or Key Compromise

If the Certification Authority's private key is compromised or is assumed to be compromised, the Certification Authority shall replace the corresponding private key of the certificate in accordance with the disaster recovery plan.

4.9.13 Circumstances for Certificate Suspension

Not applicable.

4.9.14 Certificate Suspension Applicant

Not applicable.

4.9.15 Certificate Suspension Procedure

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Features of Certificate Status Service

Not applicable.

4.10.2 Availability of Certificate Status Service

Not applicable.

4.10.3 Other Operational Features of Certificate Status Service

Not applicable.

4.11 Cancellation and Termination of Certification Service

Certification service can cancel or terminate its certificate subscription through the following:
O When the Certification Authority suspends operation
O When all certificates issued by the Certification Authority are revoked without a key change
O When a certificate is revoked by a subscriber or a certificate is expired

4.12 Key Escrow and Recovery

Not applicable.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy

Not applicable.

5. PROTECTION MEASURES FOR FACILITIES AND EQUIPMENT FOR CERTIFICATION WORK

5.1 Physical Controls

5.1.1 Site Location and Construction

The Certification Authority shall establish and operate a certification system in a separate restricted area, and the concerned system shall be established within a secured cabinet for a physical access control.
The system of Root CA shall be installed with an electromagnetic control device.

5.1.2 Physical Access Controls

The Certification Authority shall protect the installation location of the certification system, etc. from physical threats, such as trespass or illegal access, etc. by outsiders.
The Certification Authority shall install and operate a surveillance system with alarm function during irregular circumstances, such as CCTV cameras, monitoring systems and intruder detection systems, etc.
The access control system of the Certification Authority shall couple multiple systems, such as identification verification card, fingerprint recognition, weight sensor, etc. to control the access to the restricted area.
The Certification Authority shall assign security personnel to perform the security duties.

5.1.3 Power and Air Conditioning

In order to prevent serious damages from power outages, the Certification Authority shall use an uninterruptable power supply.
The Certification Authority shall install a thermo-hygrostat to maintain constant temperature and humidity.

5.1.4 Flood Controls

The Certification Authority shall install the certification system removed from the floor to protect from flooding.

5.1.5 Fire Prevention and Protection

The Certification Authority shall install fire detectors, portable fire extinguishers and fixed fire-fighting systems in the certification system room, etc.

5.1.6 Media Storage

The Certification Authority shall physically control the important storage and recording medias by storing in a safe, etc.

5.1.7 Waste Disposal

The Certification Authority shall physically destroy the documents, diskettes, etc.

5.1.8 Off-Site Backup

The Certification Authority shall physically backup the certificate, certificate suspension and certificate revocation list, etc. issued by the certification center in a physically isolated off-site and shall retain for 10 years from the date the concerned certificates become invalid. The Certification Authority shall control access for a secure operation of the off-site backup facilities by installing CCTV cameras and biometric authentication devices.

5.2 Procedural Controls

5.2.1 Principle Task Operator

The Certification Authority shall define and perform the tasks as follows in order to secure safety and reliability of the certification works.

O Policy Manager
O Certification Works Operating Manager
O Certification System Operator
O Security Supervisor
O Security Manager

The Certification Authority shall separate the functions of the policy manager, certification works operating manager, security supervisor and security manger to secure safety and reliability of the certification works.

5.2.2 Number of Principle Task Operator

The key generating tasks shall be performed jointly by 3 or more people, and other certification tasks shall be performed jointly by 2 or more people.

5.2.3 Identification and Authentication for Each Principle Task Operator

Not applicable.

5.2.4 Separation of Duties by Principle Tasks

To ensure the safety and reliability of the certification work, the Certification Authority performs the tasks separately by role.

5.3 Personnel Security Controls

5.3.1 Qualification Requirements

Requirements on the qualification, identification verification procedures and education, etc. on the certification work personnel shall be stipulated separately in internal regulations.

5.3.2 Identification Procedure

The Certification Authority shall verify the necessary matters during the hiring pursuant to the information security policy or HR(Human Resources) policy of the company.

5.3.3 Education and Training

All employees responsible for the certification works shall complete the following internal management procedure for security regulations and technical training necessary for the work performance.

O Overview and status of the certification center
O Roles and responsibilities of personnel responsible for certification works
O Overview of PKI

O Information security, etc.

5.3.4 Re-education and Training

All employees responsible for the certification works shall complete training necessary for the performance of the tasks each year.

5.3.5 Job Rotation and Movement

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Personnel conducting unauthorized actions shall be sanctioned pursuant to relevant regulations.

5.3.7 Independent Contract Personnel Requirements

Not applicable.

5.3.8 Document Disclosure to Personnel

Personnel performing the certification works may access the internal documents necessary for the performance of the responsible tasks.

5.4 Audit Log

5.4.1 Audit Log Types

The Certification Authority shall record the events on the system that supports the registration information management, private key generation and management and certification generation, issuance, authentication and time-stamping (hereinafter referred to as the “Certification System”).

The Certification Authority shall manage an audit log on the following important matters.
O Managing the key life-cycle of the Certification Authority
O Managing the certificate life-cycle
O Start and end of core certification system
O Major activities of the core certification system manager
O Security-related events, etc.

5.4.2 Period for Audit Log Processing

At least once a month, Audit logs are reviewed by security auditors for verification of the integrity of audit logs and unauthorized activities.

5.4.3 Retention Period for Audit Log

The Certification Authority shall retain the audit log for 10 years from the event date. The Certification Authority shall retain the audit log by each type and considering the availability of the storage spaces and efficiency of the management.

5.4.4 Protection of Audit Log

The audit log shall be generally managed by the security supervisor, and the manager of each task of the system shall only access the audit records on the concerned tasks.

5.4.5 Audit Log Backup Procedures

The Certification Authority conducts a daily backup on all changed information, and the backups are conducted weekly for the overall audit log.

5.4.6 Audit Log Collection System

The audit log shall be generated and stored in the internal system.

5.4.7 Notification to Audit Log Subjects

A separate notification in relation to the performance of an audit shall not be provided to individuals and business operators who caused the audit log event.
The managers responsible for the tasks shall be notified, without delay, upon occurrence of a security violation event.

5.4.8 Vulnerability Assessments

The Certification Authority shall conduct regular internal assessment for efficient security management in performing the duties.

5.5 Records Retention

5.5.1 Types of Records Retention Target

The Certification Authority shall record and retain the information related to the following duties.
O Certification works, such as issuance and management, etc. of certificates of the Certification Authority
O Operating works, such as core certification system, etc. of the Certification Authority

5.5.2 Records Retention Period

The Certification Authority shall retain the records for 10 years from the event date.

5.5.3 Records Retention Protection

The Certification Authority shall designate an employee of the Certification Authority as a document manager pursuant to the internal regulations on the certification works, and the document manager shall manage all archives. Other managers shall only access the records within the scope of his/her duties.

The Certification Authority shall protect the records as follows to prevent forgery, falsification and damage, etc. of the archives.
O Securely store the digital messages with digital signatures
O Store the general documents in a cabinet with locking devices

5.5.4 Records Retention Backup Procedures

Digitalized archives of the Certification Authority shall be stored in a separate media by using backup devices.

5.5.5 Requirements for Time-Stamping of Records Retention

Not applicable.

5.5.6 Records Retention Collection System

The records shall be created and stored in the internal system.

5.5.7 Records Retention Verification Procedures

Only the document manager shall access the records retained.
Verification procedures on the records shall be pursuant to the internal procedures of the Certification Authority.

5.6 Key Replacement

Upon expiration of the key of the certification system, loss of signature key password or damage to the key, etc., the certification system shall change the key with the same function and authority. The key replacement shall be performed with the same procedure as issuing a new key.

5.7 Failure and Disaster Recovery

5.7.1 Measure for the occurrence of failure on system resources and software

The Certification Authority recovers infrastructure and computer equipment in accordance with the disaster recovery plan in the event of a disaster that poses a serious risk to the certification system's work.

5.7.2 Measures for the destruction of system resources, software, and data

In case of damage or loss of major data such as Certification Authority's certificate, the Certification authority shall recover the data using the preserved data. Repair spares available resources if system resources and software are damaged.

5.7.3 Recovery procedure for loss of private key

A backup copy of the private key kept in the storage facility of the Certification Authority shall be used for the certification service. If the private key is assumed to be compromised, the service suspension is reported in accordance with the service suspension announcement procedure, and the Certification Authority re-issues the private key of the Certification Authority and re-issues all keys issued to individuals and businesses as a result.

5.7.4 Business Continuity Planning

The Certification Authority shall establish a business continuity plan to prevent the issuance, renewal and revocation of certificates, management tasks such as private keys, inspection tasks, and core/major tasks such as information and facility asset failures, terrorism, power outage, earthquake, fire, and weather damage. Implemented a business continuity plan, by suggesting the most efficient action to take at the point of loss on humane and physical resource, Certification Authority minimizes the interrupted time period on Certification Authority's operation work and electronic sign authority management core operation.

5.8 CA or RA Termination

Suspending or terminating the certification services of the Certification Authority shall be proceeded by minimizing the effects on the concerned actions. The following are the major performance matters.
O Provide a realistic and reasonable prior notification to all subscribers
O Maintain audit logs and archives required by the CPS for at least 1 year
O Revoke all certificates valid prior to the operating suspension

6. TECHNICAL PROTECTION

6.1 Private Key Generation and Procedure

6.1.1 Procedure for generating private key

The Certification Authority generates keys in accordance with the key generation procedure. The Certification Authority generates keys in a secure key generation system that is not connected to internal and external communications networks and is protected from physical breaches, or in hardware security modules (HSMs) that certified FIPS 140-2 Level 3. The key generation operation is conducted with the participation of at least three authorized persons.

Subscribers can generate key pairs through subscriber software provided by Korea Information Certificate Authority.

For certificate subscriber key pairs for AATL digital signature use, it is produced by the Hardware Security Module (HSM) which certified FIPS 140-2 Level 2.

6.1.2 Private Key Delivery

Private key need not be delivered to the subscriber.

.

6.1.3 Public Key Delivery

The Certification Authority shall submit the CSR in PKCS#10 format to the highest certification authority, Root CA.

6.1.4 Delivery of Public Key of Root CA

The public key of the Certification Authority shall be digitally signed by the highest certification authority, Root CA, operated by the Certification Authority. In order for the certificate of the Certification Authority to be delivered to the trusted party, a procedure to deliver the certificate of the Certification Authority to be delivered when the applicant accepts the issued certificate shall be established and implemented.

6.1.5 Private Key Length

The key length of the root certification authority operated by the Certification Authority is RSA 4096 bits, the key length of the Certification Authority is 2048 bits, and the key length of the subscriber certificate is 2048 bits. The algorithms used to generate the keys are as follows:

O algorithm: RSA
O hash algorism: SHA-256

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Private Key Usage

Certificate of the Certification Authority and the subscriber certificate shall be used for digital signatures. Purposes of the key usage shall be stipulated in the extended key usage field of the subscriber certificate. The concerned matters shall reference the “Certification Center Certificate Profile Standard.”

6.2 Private Key Protection and Encryption Module

6.2.1 Private Key Storage

The Certification Authority key pair is stored and operated in the Hardware Security Module (HSM), which certified FIPS 140-2 Level 3.

6.2.2 Private Key Multi-Person Control

The Certification Authority shall perform the Certification Authority key pair generation pursuant to the internal key generation procedures. When generating key pairs, at least 3 people or more shall participate.

6.2.3 Private Key Escrow

The Certification Authority shall not delegate the key pair of the Certification Authority to a third party.

6.2.4 Private Key Backup

The private key of the Certification Authority shall be kept at a secure location according to the backup procedures. The private key backup shall be stored in an encrypted device token of FIPS 140-2 level 3 or higher, and the concerned token shall be securely stored within a fire-resistant safe.

6.2.5 Private Key Retention

The Certification Authority shall not store a private key of the Certification Authority that has expired.

6.2.6 Private Key Extraction

The private key of the Certification Authority shall be extracted with encryption by using Hardware Security Module (HSM) only for backup purposes.

6.2.7 Private Key Storage

The private key of the Certification Authority shall be stored with Hardware Security Module (HSM) through encryption.

6.2.8 Private Key Activation

The private key of the Certification Authority may be activated under two factor authentication by 2 or more operators.

6.2.9 Private Key Deactivation

The private key of the Certification Authority may be deactivated under two factor authentication by 2 or more operators.

6.2.10 Method of Destroying Private Key

The Certification Authority may destroy the private key of the Certification Authority for the following reasons and shall be deleted in the Hardware Security Module (HSM), along with

the backed-up private key.
O The certificate of the Certification Authority has expired
O The private key of the Certification Authority has been, or may be, damaged or leaked

The subscriber may delete the private key and certificate of the subscriber by directly accessing the website when the private key of the subscriber is no longer needed.

6.2.11 Cryptographic Module Rating

Refer to Article 6.2.1 of this document.

6.3 Management of Key Pair

6.3.1 Public Key Retention

The public key shall be stored in the database of the Certification Authority during the period stipulated in Article 5.5.2 of this document.

6.3.2 Expiration Date of Certificate

The effective period of the certificate shall expire on the expiration date stipulated in the certificate field. The effective periods of the certificates of the Certification Authority and subscriber are as follows.
O Certificate for the Certification Authority: 10 years
O Certificate for Online Certificate Status Protocol (OCSP): 10 years
O Certificate for Time Stamp Authority (TSA): 10 years
O User Certificate: 1 year, 2 years, 3 years

6.4 Activation Data

The activation data shall be the information necessary to operate and use the Hardware Security Module (HSM). The activation data shall have operating key and password, etc.

6.4.1 Activation Data Generation

The activation data shall be generated according to the specification of the Hardware Security Module (HSM).

6.4.2 Activation Data Protection

The activation data shall be protected by the operating key and password. Key for access authentication shall be maintained by designated managers.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

6.5.1 Particular computer security requirements

System information of Certification Authority is protected by server and OS control, physical control, and network control.

6.5.2 System Security Requirement

System of the Certification Authority satisfies the ISO-27001 requirements.

6.6 Life Cycle Security

6.6.1 System Development Controls

Changing the function and improving the performance of the certification system shall be conducted under the approval of the certification works policy manager or operating manager.

6.6.2 Security Management Controls

All computers that access the certification system are properly separated by each of functions and operated with minimal access.

6.6.3 Life Cycle Security Controls

Not applicable.

6.7 Network Security Controls

Certificate authority uses intrusion detection systems and intrusion prevention systems for network security.

6.8 Time-Stamping

The time of Certification Authority’s system uses NTP.

7. CERTIFICATE PROFILE

7.1 Certificate Profile

Certificates issued by the certificate authority shall comply with RFC 5280.

7.1.1 Certificate Version

Issue the X.509 version3 certificate. (specify version field value as number 2)

7.1.2 Certificate Extensions

Matters such as whether to use extended fields of certificates shall follow the 「The Certification Center Certificate Profile Standard」.

7.1.3 Algorithm Object Identifiers

The Algorithm Object Identifiers used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.1.4 Name Forms

The Name Forms used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.1.5 Name Constraints

The Name Constraints used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.1.6 Certificate Policy Object Identifier

The Certificate Policy Object Identifier used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.1.7 Certificate Policy Constraints Extension

The Certificate Policy Constraints Extension used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.1.8 Certificate Policy Qualifiers Syntax and Semantics

The Certificate Policy Qualifiers Syntax and Semantics used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.1.9 Semantics and Processing for the Certificate Policies Extension

The Semantics and Processing for the Certificate Policies Extension used for certificates follows 「The Certification Center Certificate Profile Standard」.

7.2 CRL Profile

7.2.1 CRL(Certificate Revocation List) Version

CRL issued by the Certification Authority shall comply with RFC 5280.

7.2.2 CRL Extended Field

The CRL Extended Field used for CRL follows 「The Certification Center Certificate Profile Standard」.

7.3 OCSP Certificate Profile

7.3.1 OCSP(Online Certificate Status Protocol) Certificate Profile Version

The OCSP Certificate Profile used for OCSP follows 「The Certification Center Certificate Profile Standard」.

7.3.2 OCSP Certificate Extended Field

The OCSP Certificate Extended Field used for OCSP follows 「The Certification Center Certificate Profile Standard」.

8. AUDIT COMPLIANCE AND OTHER ASSESSMENTS

The Certification Authority shall comply with domestic and international legal systems and related technical standards for safe operation of the certification system, and conduct regular audits by independent third parties.

8.1 Frequency and Environment of Audit

Certification Practice Statement, facilities and equipment shall be audited annually.

8.2 Subject and Qualification of Audit

Audits shall be performed by qualified and skilled personnel as follows.
① An independent person from the audited organization
② A person with sufficient knowledge of domestic and international legal systems and related technical standards
③ Specialist on PKI Technology, Information and Communication Technology and Information System Audit
④ International Qualified WebTrust or equivalent;

8.3 Auditor's Relationship to audit targets

The Certification Authority shall identify and participate in the verification and operation of an independent auditor with no role or responsibility, and shall have no financial or business interest with the auditor.

8.4 Scope of Audit

The Audit includes quality assurance system of certification service provided by Certification Authority, compliance with the Certification Authority regulations, key management of the Certification Authority, and certificate management for the scope of assessment.
O Inspection on the safety operation of facilities and equipment related to certification work
O Preparation of audit items and preparation of evidence, etc.
O Method: Check that the following inspection areas comply with the work procedures
① Certification service
② Managing electronic signature keys
③ Other certifications and services
④ Management of facilities and equipment
⑤ Management of documents and records
⑥ Test operation and information provision
⑦ Network and System Security
⑧ Physical Security
⑨ Disaster prevention
⑩ Managed Security and Emergency Planning

8.5 Action Based on Audit Results

Any deficiencies and anomalies found through the audit are included in the report and policy and technical actions are taken according to the audit results.

8.6 Announcement of Audit Results

The auditor reports the audit results to the Certification Authority, and the Certification Authority publishes a summary of the audit results and related information on the website.

9. OTHER ITEMS SUCH AS CERTIFICATION WORK GUARANTEE

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The Certification Authority may levy fees to the applicants for issuance and renewal of certificates.

9.1.2 Certificate Access Fee

The Certification Authority may levy fees to the subscribers or trusted parties accessing and verifying the certificates.

9.1.3 Certificate Suspension and Revocation List Access Fees

The Certification Authority may levy fees to the subscribers or trusted parties accessing the certificate suspension and/or revocation list.

9.1.4 Fees for Other Services

The Certification Authority may provide additional services related to the certificates, such as online certificate status protocol (OSCP), time-stamping authority (TSA), etc., and may levy fees for such services.

9.2 Financial Responsibility

The Certification Authority shall indemnify only the subscriber or the user who trusts the certificate for damages in connection with the performance of the certification work. However, in the event that the damage is caused by force majeure or if the Certification Authority proves that the damage is not culpable, the liability for compensation shall be exempted.

9.2.1 Insurance Coverage

The Certification Authority shall subscribes and maintains liability insurance.

9.2.2 Other Assets

Financial information of Certification Authority, KICA, is open to the public.

9.3 Confidentiality of Business Information

The Certification Authority shall securely protect the information obtained and generated in relation to the certification services. Information that can hinder the safety and reliability of the certification services and confidential information applicable as secrets requiring legal protection, such as business secrets, etc., shall be managed under confidentiality, and the confidential information shall be protected securely.

9.3.1 Scope of Confidential Information

Not applicable.

9.3.2 Information Not Within the Scope of Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Confidential Information

Not applicable.

9.4 Privacy of Personal Information

The Certification Authority has established and is managing a “privacy policy” in relation to the personal information protection, and such “privacy policy” shall be posted on the website.
The Certification Authority shall comply with the relevant laws, such as the Information and Communications Networks Act, Personal Information Protection Act of Korea, etc., to protect the personal information provided by the customers and shall establish and implement a privacy policy.
The Certification Authority shall destroy the personal information when such personal information collected achieve the purposes of processing or are no longer necessary, or shall store and manage the concerned personal information or the personal information file, when required to retain pursuant to relevant laws.

9.4.1 Privacy Plan

The Certification Authority shall comply with the relevant laws and regulations, such as the Personal Information Protection Act, and shall collect, retain and process the personal information pursuant to the privacy policy posted on the webpage.

9.4.2 Privacy Criteria

The personal information shall be collected and retained pursuant to the privacy policy posted on the website.

9.4.3 Privacy Exceptions

Not applicable.

9.4.4 Responsibility to Protect Private Information

The Certification Authority complies with the related laws and regulations, such as the Personal Information Protection Act, and collects, retains, and processes the personal information processing policies posted on the website.

9.4.5 Notice and Consent to Use Private Information

The Certification Authority shall comply with the relevant laws and regulations, such as the Personal Information Protection Act, etc., and shall provide notification on the use of the personal information and collect consent of the data subject from the website and the application.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Not applicable.

9.4.7 Other Information Disclosure Criteria

Not applicable.

9.5 Intellectual Property Rights

All intellectual property rights derived from this certification works shall be the property of the Certification Authority and may not be legally used without a permission separately stipulated by the Certification Authority.

9.6 Warranty Responsibilities

The Certification Authority verifies the facts of the information submitted by the subscriber only for the minimum amount of information necessary to provide the service and warranties to the user the factuality of such information.

9.6.1 Certification Authority Warranties

Not applicable.

9.6.2 Registration Authority Warranties

Not applicable.

9.6.3 Subscriber Warranties

Not applicable.

9.7 Disclaimers of Warranties

The Certification Authority shall withdraw the warranties when the subscriber applies for the issuance of the certificate through improper means or when the certificate is taken.

9.8 Limitations of Liability

The Certification Authority's liability may be limited or exempted for the following cases.

A) Damages from using the certificate by changing the usage by the subscriber at his/her discretion
B) Damages from reasons not attributable to the Certification Authority, such as communications disorder or subscriber system error, etc. during the process of providing certification services, such as issuance (new, renewal) of certificate, certificate suspension and revocation list notification, etc.
C) Damages from negligent or intentional fault of the subscriber
D) Damages from emergency, such as war, natural disasters, etc.
E) Damages from policy change of the government
F) Other damages incurred without the fault of the Certification Authority

9.9 Effect of CPS

This CPS shall become effective when posted on the website, and amendments shall be posted on the website 10 days prior to the effective date of such amendment.

9.10 Communication and Notification

This CPS shall be posted on the website. Persons intending to make notifications, demands or

requests in relation to this CPS shall contact the following.
O URL: trust.signgate.com
O E-mail: webmaster@signgate.com
O Phone: +82-2-360-3251

9.11 Amendments

9.11.1 Procedure for Amendment

The Certification Authority may make minute amendments or correct errors, etc. unrelated to the policy of the CPS without prior notification. When the Certification Authority amends the CPS from changes in the important certification policy, such changes shall be posted on the website 10 days prior to the implementation for the subscribers, etc. to verify the information through an internal approval procedure.

9.11.2 Notification of Amendment

The Certification Authority shall post the amended CPS on the website when amending the CPS.

9.12 Dispute Resolution

9.12.1 Governing Law and Trial Jurisdiction

This CPS shall be interpreted and construed pursuant to the relevant laws of Korea, and Seoul Central District Court shall have jurisdiction on the first instance.