

Certification Practice Statement

Ver. 1.5

Sep 2009



Contents

1. Outline	1
1.1 Background & Purpose	1
1.1.1 Electronic Signature Certification System	1
1.1.2 Certification Practice Statement	1
1.1.3 Introduction of Korea Internet & Security Agency	1
1.2 Name of Certification Practice Statement	2
1.3 Electronic Signature Certification System Concerned Authorities	2
1.3.1 Information Security Promotion Subcommittee	2
1.3.2 National Intelligence Service	2
1.3.3 Ministry of Public Administration and Security	2
1.3.4 Korea Internet & Security Agency	2
1.3.5 Certification Authority	4
1.3.6 Relying Party	7
1.4 Certification Practice Statement Management	7
1.4.1 Certification Practice Statement Establishers and Revisers	7
1.4.2 Revision Procedures	8
1.4.3 Enforcement Procedures	8
1.5 Definitions & Abbreviations	9
2. Certificate Types and Fees	12
2.1 Certificate Types	12
2.1.1 Certificate Policy	12
2.1.2 Certificate Scope and Usage	12
2.2 Certification Service Fee	12
2.2.1 Fees for the Issue, Reissue and Renewal Issue of Certificates	13
2.2.2 Certificate Access Fee	13
2.2.3 Certificate Revocation List Access Fee	13
2.2.4 Fees for Other Services	13

3. Issue of Certificates and Certification Practice	14
3.1 Applying For the Issue of Certificates	14
3.1.1 Use of Names	14
3.1.2 Information On the Issue of Certificates	14
3.1.3 Certificate Validity Period	14
3.1.4 Receipt of Certificates	15
3.2 New Issue of Certificates	15
3.2.1 Identity Check for Certification Authorities and Certificate Applicants	15
3.2.2 New Issue Procedures	15
3.3 Renewal Issue of Certificates	16
3.3.1 Identity Check in Renewal Issue	16
3.3.2 Renewal Procedures	16
3.4 Reissue of Certificates	17
3.4.1 Identity Check in Reissue	17
3.4.2 Reissue Procedures	17
3.5 Change of Subscriber Registration Information	17
3.6 Suspension, Revival, and Revocation of Certificates	17
3.6.1 Identity Check in Application for Suspension, Revival, and Revocation	17
.....	
3.6.2 Certificate Suspension	18
3.6.3 Certificate Revival	18
3.6.4 Certificate Revocation	19
3.7 Certificate Validity Check Service (OCSP)	20
3.8 Other Additional Services	20
3.9 Certificate Profile	20
3.10 Certificate Revocation List (CRL) Profile	21

3.11 Certificate Profile for OCSP Service	21
3.12 Renewal of Electronic Signature Keys	21
3.13 Suspension and Revocation of Certification Practice	22
3.14 Suspension or Cancellation of Certification Practice	22
4. Announcement of Information Related to Certification Practice	23
4.1 Announcement System	23
4.2 Announcement Method	23
5. Certification Practice System and Equipment Protection Measures	24
5.1 Physical Protection Measures	24
5.1.1 Physical Access Control	24
5.1.2 Power Supply	24
5.1.3 Flood Control	24
5.1.4 Fire Prevention	24
5.1.5 Storing Media	25
5.1.6 Waster Handling	25
5.1.7 Long-Distance Backup	25
5.2 Procedural Protection Actions	25
5.2.1 Work Classification by Role	25
5.2.2 Personnel by Main Work	25
5.3 Technical Protection Actions	25
5.3.1 Creation of Electronic Signature Keys	25
5.3.2 Key Size and Hash Value	26
5.3.3 Device for Storing Electronic Signature Creation Keys	26
5.3.4 How to Delete and Destroy Electronic Signature Creation Keys ..	26
5.3.5 Electronic Signature Creation Keys Use Period	26
5.3.6 Computer and Network Security Control	26

5.4 Personnel Security	27
5.5 Audit Data	27
5.5.1 Types of Cases in Audit Data	27
5.5.2 Review and Protection of Audit Data	27
5.5.3 Notification of the Occurrence of Cases	27
5.6 Archiving	27
5.6.1 Types of Objects of Archiving	27
5.6.2 Protection of Archives	28
5.7 Recovery from Glitches and Disasters	28
5.7.1 Countermeasures on the Occurrence of Glitches in System Sources and Software	28
5.7.2 Countermeasures on Damaged and Destroyed Data	28
6. Miscellaneous Provisions Including Certification Practice Guarantee - 29	
6.1 Guarantee	29
6.1.1 Liability for Guarantee	29
6.1.2 Exemptions	29
6.2 Dispute Resolution	29
6.2.1 Observance Laws	29
6.2.2 Jurisdiction	29
6.2.3 Dispute Mediation	29
6.3 Private Information Protection	30
6.4 Audit and Check	30
6.4.1 Security Check	30
6.4.2 Observance of Security Practice Regulations	30
6.5 Observance of Relevant Laws	30
6.6 Validity of Certification Practice Statement	31

1. Outline

1.1 Background & Purpose

1.1.1 Electronic Signature Certification System

The Electronic Signature Law (Law Issue No.: 5792), which was enacted on February 5, 1999 and became effective on July 1, 1999, aims to promote an information-oriented society and improving convenience for citizens by specifying basic items regarding the establishment and operation of an electronic signature certification management system and a national public key infrastructure, in order to ensure the security and reliability of electronic data which are processed via open information networks, such as the Internet, etc., and to activate the use of such networks.

1.1.2 Certification Practice Statement

The purpose of the Korea Internet & Security Agency's (hereinafter referred to as "KISA") Certification Practice Statement is to provide matters necessary for the tasks related to electronic signature certification, such as the KISA's certificate policy, the issue and management of certificates, security control, and other operational policies and procedures, in accordance with the Electronic Signature Law, the Electronic Signature Law's Enforcement Ordinance (hereinafter referred to as "Enforcement Ordinance"), the Electronic Signature Law's Enforcement Regulations (hereinafter referred to as "Enforcement Regulations") and all other laws related to the responsibilities and duties of the KISA and other certification authorities.

1.1.3 Introduction of KISA

The KISA has provisions relating to its establishment in accordance with Provision 1 of Article 52 of the Law on Information Communication Network Use Promotion and Information Protection. As a top-level certification authority in the electronic signature certification management system, its main duties include the research and development of the policies and technologies required for information security, to enable the sound, orderly and secure communication of information, and the promotion of an information-oriented society to increase the convenience of people's lives, in accordance with the provisions of Article 25 of the Electronic Signature Law.

1.1.3.1 Certification Practice Related Contact Information

The KISA's certification practice related contact information are as follows.

- o URL: <http://www.rootca.or.kr>
- o E-mail: rootca@kisa.or.kr
- o Address: Korea Internet & Security Agency, 4th floor, IT Venture Tower, 78, Garak-dong, Songpa-gu, Seoul
- o Telephone: 82-2-4055-411

1.1.3.2 Certification Practice Related Information

The KISA's certification practice related information are as follows.

- o The KISA's Certification Practice Statement: <http://www.rootca.or.kr/rca/cps.htm>
- o Certification Authority List: <http://www.rootca.or.kr/lca/lca.htm>
- o Certificate List: <http://www.rootca.or.kr/cert.htm>
- o Certificate Revocation List: <http://www.rootca.or.kr/crl.htm>

1.2 Name of Certification Practice Statement

This document is named 'Certification Practice Statement of Korea Internet & Security Agency's Top-Level Certification Authority.'

1.3 Electronic Signature Certification System Concerned Authorities

1.3.1 Information Security Promotion Subcommittee

- o Deliberates a policy on the establishment and operation of a national public key infrastructure.
- o Deliberates plans for the establishment of a cross-certification system between nations.

1.3.2 National Intelligence Service

- o Deliberates whether the results of an actual audit during the designation of a certification authority in national agencies and local autonomous entities agree with the national security policy.
- o Guides the KISA's security in its certification practice.
- o If a national agency or local autonomous entity is designated as a certification authority, the National Intelligence Service shall guide the corresponding certification authority's security in its certification practice.

1.3.3 Ministry of Public Administration and Security

The Ministry of Public Administration and Security is a policy-making and supervision agency, which carries out the following activities to ensure the secure and reliable operation of the electronic signature certification system:

- o Establishing policy for building and operating the electronic signature certification system in a secure and reliable manner.
- o Designating a certification authority, correction order, work suspension, and cancellation of designation and work investigation.
- o Managing and supervising the KISA's and certification authorities' observance of the Electronic Signature Law, and its Enforcement Ordinances and Enforcement Regulations.
- o Cross-recognition of electronic signatures between foreign governments.

1.3.4 KISA

According to the provisions of Articles 10, 12, and 25 of the Electronic Signature Law, the KISA shall carry out its duties and roles as a top-level certification authority in the electronic signature certification management system, including the following:

- o Establishing and operating a secure electronic signature certification management system
- o Undertaking the certificates of subscribers to certification authorities which have had their certification revoked
- o Undertaking the certificates of subscribers to certification authorities which have had their designation cancelled

- o Performing investigations for the designation of certifying authorities
- o Inspecting certification authorities, and supporting their secure operation
- o Developing and distributing electronic signature certification technology
- o International cooperation and support, such as cross-recognition, etc.
- o Other tasks related to electronic signature certification
- o Certification practice, such as a certification authority's certification on electronic signature verification keys, etc.
- o Issuing the Certificate Revocation List
- o Time-stamping

The KISA's duties are as follows.

1.3.4.1 Provision and Notification of Correct Information

The KISA shall notify certification authorities and the relying parties of the following information that may have an effect on the reliability or validity of a certificate, so that it can be confirmed by anyone under the electronic signature certification system:

- o Certificate Information
 - Certificate
 - Certificate Revocation List
- o Other information related to the performance of certification practice

1.3.4.2 Countermeasures to Improper Electronic Signature Creation Keys

If the KISA recognizes that its electronic signature creation keys being used for certification practices are not secure, the KISA shall revoke such certificates, including the electronic signature verification keys with the appropriate electronic signature creation keys, and shall reissue the certificates by creating new electronic signature keys. After renewing and reissuing the certificates of the certification authorities by using new electronic signature creation keys, the KISA shall promptly announce the fact so it can be confirmed by anyone in the certification management system, and so that countermeasures can be considered for ensuring the security and reliability of certification practice.

If the KISA is notified by a certification authority that electronic signature creation keys

are lost, damaged, stolen, leaked, or weak, the KISA shall revoke the certificate that was issued to the appropriate certification authority and then will promptly announce the fact so that it can be easily confirmed by anyone in the certification management system. If the KISA is notified by a certification authority under the management of a national agency or a local autonomous entity that electronic signature creation keys have been lost, damaged, stolen, leaked, or are weak, the KISA shall promptly notify the chief of the National Intelligence Service.

1.3.4.3 Countermeasures to Vulnerability in the Electronic Signature Algorithm

If the KISA recognizes that an electronic signature algorithm being used in certification practice is not secure, the KISA shall revoke all certificates and certificates held by certification authorities that were issued using said electronic signature algorithm, and will then promptly announce the fact so that it can be easily confirmed by anyone in the certification management system, and shall consider countermeasures for ensuring the security and reliability of certification practice.

If the KISA is notified of a vulnerability in the electronic signature algorithm by a certification authority, the KISA shall revoke the certificate which was issued to the appropriate certification authority, and then shall promptly announce the fact so that it can be confirmed by anyone in the certification management system. If the KISA is notified of the vulnerability in the electronic signature algorithm by a certification authority under the management of a national agency or a local autonomous entity, the KISA shall promptly notify the chief of the National Intelligence Service of the same.

1.3.5 Certification Authority

A certification authority is a national agency, local autonomous entity, or corporation that has been designated in accordance with the provisions of Article 4 of the Electronic Signature Law, and which provides subscribers with the following certification services. It should be noted that any party corresponding to the reasons for disqualification provided in Article 5 of the Electronic Signature Law cannot be designated as a certification authority.

- o Identity check
- o Issuing a certificate
- o Certificate suspension and revocation

- o Renewing a certificate
- o Giving public notification of certificate-related information
- o Time-stamping, etc.

A certification authority's duties are as follows.

1.3.5.1 Provision and Notification of Correct Information

A certification authority shall provide the KISA with the correct information and facts, in the following cases:

- o when a certificate is issued
- o when a certificate is suspended or revoked
- o when a certificate is reinstated

A certification authority shall promptly notify subscribers and relying parties of the following information that may have an effect on the reliability or validity of a certificate, so that it can be confirmed by anyone in the certification management system:

- o [Suspension or revocation of a certification authority's certification ability](#)
- o [Information on a certificate](#)
 - [A subscriber's certificate](#)
 - [A subscriber's certificate revocation list](#)
- o [Other information related to the performance of certification practice, etc.](#)

1.3.5.2 Protection of Electronic Signature Creation Keys

A certification authority shall create its own electronic signature keys in a secure manner by using reliable software or hardware, and shall securely manage the electronic signature creation keys by using a security module that satisfies the technical standards provided in the Rule on Certification Authorities' Installation and Devices, so that such electronic signature keys cannot be lost, damaged, stolen or leaked.

If a certification authority creates an electronic signature key for a subscriber, the certification authority shall do so through a secure method by using reliable software or hardware. In addition, the certification authority shall code the subscriber's electronic

signature key and then store it in a storage device in accordance with the password algorithm specified in Item 3 of Provision 1 of Article 5 of the Rule on Certification Authorities' Installation and Devices. To ensure the integrity of electronic signature creation keys, the certification authority shall also store other information, such as Message Authentication Code (MAC), etc. which it shall directly deliver to the subscriber.

1.3.5.3 Use of Certified Electronic Signature Creation Keys

When providing certification services, a certification authority shall use electronic signature creation keys according to the electronic signature verification keys certified by the KISA.

1.3.5.4 Notification of Lost, Damaged, Stolen or Leaked Electronic Signature Creation Keys & Actions

If the electronic signature creation keys of a certification authority are lost, damaged, stolen or leaked, the certification authority shall promptly notify the KISA of the fact and then consider countermeasures to ensure the security and reliability of its certification practice, in accordance with Provision 3 of Article 21 of the Electronic Signature Law.

1.3.5.5 Notification of Vulnerability in Electronic Signature Creation Keys & Actions

If a certification authority recognizes that its electronic signature creation keys are not secure, the certification authority shall promptly notify the KISA of the fact, and then shall consider countermeasures to ensure the security and reliability of its certification practice.

1.3.5.6 Notification of Vulnerability in Electronic Signature Algorithm & Actions

If a certification authority recognizes that its electronic signature algorithm is not secure, the certification authority shall promptly notify the KISA of the fact and then shall consider countermeasures to ensure the security and reliability of its certification practice.

1.3.6 Relying Party

Relying parties are parties that rely on and use certificates issued by the KISA, and include the following:

- o Certification authorities
- o Subscribers to certification authorities
- o Foreign certification authorities which have entered into a cross-recognition arrangement, in accordance with Provision 2 of Article 27 of the Electronic Signature Law
- o Subscribers to foreign certification authorities which have entered into a cross-recognition arrangement, in accordance with Provision 2 of Article 27 of the Electronic Signature Law, etc.

The duties of relying parties are as follows.

1.3.6.1 Understanding the Purpose of Using Certificates

A relying party shall understand the purpose of using a certificate issued by the KISA, as specified in 2.1.2 Scope and Usage of Certificates in this Certification Practice Statement.

1.3.6.2 Certificate Verification

A relying party shall verify the appropriate certificate's validity period, scope and usage, authenticity, etc., before using the certificate.

1.3.6.3 Verification of Certificate Suspension and Revocation

A relying party shall verify the validity of the appropriate certificate via the certificate suspension and revocation list before using the certificate.

1.4 Certification Practice Statement Management

1.4.1 Certification Practice Statement Establisher/Reviser

The establisher or reviser of this Certification Practice Statement is the chief of the KISA. In the event of establishment or revision, the establisher or reviser shall report to the Minister of Public Administration and Security in accordance with Provision 1 of Article 6 and Provision 2 of Article 25 of the Electronic Signature Law.

1.4.2 Revision Procedures

If the Minister of Public Administration and Security orders the KISA to make changes to the Certification Practice Statement, the KISA shall revise the same in accordance with Provision 2 of Article 6 and Provision 2 of Article 25 of the Electronic Signature Law.

If the chief of the KISA judges that the Certification Practice Statement needs to be changed, the Certification Practice Statement shall be revised.

The KISA shall maintain and manage documents related to the revision of the Certification Practice Statement, which shall include the following:

- o Certification Practice Statement versions
- o Outlines of application practice and scope
- o Documents on the revision of Certification Practice Statement
 - Revised provisions in the existing Certification Practice Statement
 - Revision details
 - Reasons for revision, etc.

1.4.3 Enforcement Procedures

The KISA shall report the established or revised Certification Practice Statement to the Minister of Public Administration and Security.

The KISA shall announce the established or revised Certification Practice Statement in '1.1.3.2 Certification Practice Related Information' of this Certification Practice Statement, and shall individually notify certification authorities of the fact of its establishment or revision.

The established or revised Certification Practice Statement shall become effective on the date of reporting.

1.5 Definitions & Abbreviations

o DN(Distinguished Name)

A type of name that is used to identify the authority that issued a certificate and the owner of a certificate. The DN must observe the technical standards provided in the Rule on Certification Authorities' Installation and Devices.

o Subscriber

A person or an entity that has a certificate on his/her/its own electronic signature verification keys issued by a certification authority

o Certification Authority

An authority that provides certification services after being designated by the Minister of Public Administration and Security, in accordance with the provisions of Article 4 of the Electronic Signature Law

o Relying Party

A person or an entity that receives the certificate from the KISA, and then relies on and uses said appropriate certificate

o Identity Check

The KISA's act of checking the authenticity of a certification authority, an applicant, and information for ensuring the reliability of a certificate when a certificate is issued, renewed, suspended, or revoked

o Real Name

The name on a certificate of residence, on a certificate for business registration, or that is designated under the Law on Real-Name Financial Transaction and Privacy Protection and its enforcement ordinance (Presidential Decree No.: 15744)

o Certification

An act of verifying the fact that electronic signature verification keys agree with the electronic signature creation keys owned by a natural person or corporation

o Electronic Signature Certification System

A system for providing certification services, including the issue of a certificate, the management of certification-related data, etc.

o Electronic Certificate

Electronic data verifying the fact that electronic signature verification keys agree with the electronic signature creation keys owned by a natural person or corporation

o Certification Practice

Practice of providing certification services, including the issue of a certificate, the management of certification-related data, etc.

o Electronic Data

Information that is generated, sent and received, or stored in an electronic form by the use of data-processing devices, such as a computer, etc.

o Electronic Signature

Data in electronic form that are created by electronic signature creation keys using an asymmetric cryptosystem, in order to verify the identity data of the person who generated the electronic data, and to verify whether the electronic data has changed or not.

o Electronic Signature Verification Key

Electronic data that are used for the verification of electronic signatures

o Electronic Signature Creation Key

Electronic data that are used for the creation of electronic signatures

o Electronic Signature Key

Electronic signature creation keys and corresponding electronic signature verification keys

o Certification System

A system that supports the management of registered data, the creation and management of electronic signature keys, the creation and issue of certificates, and time-stamping.

2. Certificate Types and Fees

2.1 Certificate Types

2.1.1 Certificate Policy

The KISA shall issue certificates to certification authorities that have been designated in accordance with the provisions of Article 4 of the Electronic Signature Law, according to Article 15 and Provision 2 of Article 25 of the Electronic Signature Law, and shall suspend or revoke said certificates according to Articles 16 or 18 and Provision 2 of Article 25 of the Electronic Signature Law.

2.1.2 Certificate Scope and Usage

Certificates that have been signed and issued by the KISA shall be used to verify the agreement of the KISA's electronic signature verification keys and the KISA's own electronic signature creation keys.

Certificates that were issued to certification authorities by the KISA shall be used to verify the agreement of those certification authorities' electronic signature verification keys and those certification authorities' own electronic signature creation keys.

If an application is made by a certification authority in accordance with Provision 4 of Article 15 and Provision 2 of Article 25 of the Electronic Signature Law, the KISA can issue one or more of the following certificates, which restrict the scope or usage of a certification authority's certificates:

Classification	Usage
Authority's Certificate	Issue of certificates for subscribers
Time-Stamping Certificate	Electronic signatures for the responses of time-stamping
OCSP Certification	Electronic signatures for the responses of OCSP

2.2 Certification Service Fee

2.2.1 Fees for the Issue, Reissue and Renewal of Certificates

If necessary, the KISA can impose fees on certification authorities that apply for the issue, reissue and renewal of certificates in accordance with the provisions of Article 28 of the Electronic Signature Law.

2.2.2 Certificate Access Fee

The KISA shall not impose any fee on a relying party that reads and checks certificates.

2.2.3 Certificate Revocation List Access Fee

The KISA shall not impose any fee on a relying party that accesses the certificate suspension and revocation list.

2.2.4 Fees for Other Services

If necessary, the KISA can impose fees for other services in accordance with the provisions of Article 28 of the Electronic Signature Law.

3. Issue of Certificates and Certification Practice

3.1 Application For the Issue of Certificates

A certification authority shall access the Security Authority's website to receive necessary data and a form, or the same shall be directly issued, filled out, and then the certification authority shall directly visit the KISA for application.

3.1.1 Use of Names

Technical standards in the Rule on Certification Authorities' Installation and Devices shall apply to the names used for basic areas in a certificate, certificate suspension and revocation list.

Authority names or corporation names shall be used for DNs in a certificate issued by the KISA.

3.1.2 Information on the Issue of Certificates

A certificate issued by the KISA shall include the following items, in accordance with Provision 2 of Article 15 and Provision 2 of Article 25 of the Electronic Signature Law:

- o Name of certificate authority
- o Certificate authority's electronic signature verification keys
- o Electronic signature type used by the KISA and certification authority
- o Certificate serial numbers
- o Certificate validity period
- o Name of the KISA as a top-level certification authority
- o Relevant matters in the event that the scope or usage of a certificate is restricted, etc.

3.1.3 Certificate Validity Period

The KISA shall determine the proper certificate validity period by considering the scope and usage of a certificate and the security and reliability of the relevant technology, in accordance with Provision 5 of Article 15 and Provision 2 of Article 25 of the Electronic

Signature Law.

- o The validity period of the KISA's certificates shall be within 20 years.
- o The validity period of the certificates for certification authorities issued by the KISA are as follows.

Classification	Key Length	
	1024bit	2048bit
Certification Authority's Certificate	Within 5 years	Within 10 years
Time-Stamping Certificate	Within 3 years	Within 10 years
OCSP Certificate	Within 3 years	Within 10 years

3.1.4 Receipt of Certificates

A certification authority shall receive its certificates in person at the KISA, or through an information communication network after the notification certificate issuance

A certification authority can use its received certificates beginning on their date of validity.

3.2 New Issue of Certificates

3.2.1 Identity Check for Certification Authorities and Certificate Applicants

The KISA shall check the identity of a certification authority via a set book for certification authorities, a certificate of business registration and a certified copy of the corporation's register, as submitted by the certification authority. For a national agency or local autonomous entity, the KISA shall check the same via the corresponding documents.

After directly having an interview with him/her, the KISA shall check the identity of a certificate applicant or his or her proxy for a certificate with the following methods:

- o As a voucher for checking the identity of an applicant or his/her proxy prescribed in Provision 3 of Article 13 of the Electronic Signature Law, checking his/her name and resident registration number in accordance with Provision 2:Identity Check Method of Article 13 of the Electronic Signature Law.
- o Conducting an identity check with a document verifying that an applicant or his/her

proxy works for the appropriate certification authority, checking whether an applicant is qualified to represent an agency or corporation, or whether his/her proxy is authorized to be the applicant's proxy.

3.2.2 New Issue Procedures

Before issuing a new certificate, the KISA shall verify the following details of an application:

- o The uniqueness of the electronic signature verification keys submitted by an applicant for a certificate
- o The agreement of the electronic signature verification keys submitted by an applicant for a certificate with the appropriate certification authority's own electronic signature creation keys.
- o The uniqueness of a DN submitted by an applicant for a certificate.

3.3 Renewal of Certificates

3.3.1 Identity Check for Renewal

If a certification authority applies for the renewal of a certificate, the KISA shall conduct an identity check in accordance with the procedures involved in an application for the new issue of a certificate.

3.3.2 Renewal Procedures

Before the actual issue, the KISA shall verify the following details of the application for the renewal of a certificate. It should be noted that certification authorities cannot apply for the renewal of certificates with the same electronic signature creation keys.

- o The uniqueness of the electronic signature verification keys submitted by an applicant for a certificate.
- o The matching of the DN submitted by an applicant for a certificate to the DN stated in a previous certificate.

3.4 Reissue of Certificates

3.4.1 Identity Check in Reissue

If a certification authority applies for the reissue of its own certificate because its validity period has expired or the certificate has been revoked, the KISA shall conduct an identity check in accordance with the procedures for an application for the new issue of a certificate.

3.4.2 Reissue Procedures

The KISA shall verify the following details of an application for the reissue of a certificate before reissuing it:

- o The uniqueness of the new electronic signature verification keys submitted by the applicant for a certificate
- o The agreement of the new electronic signature verification keys submitted by the applicant for a certificate with the appropriate certification authority's own electronic signature creation keys.
- o The uniqueness or identity of a DN submitted by an applicant for a certificate.

3.5 Change of Subscriber Registration Information

This is not applicable.

3.6 Suspension, Revival, and Revocation of Certificates

3.6.1 Identity Check in Application for Suspension, Revival, or Revocation

If a certification authority applies for the suspension, revival, or revocation of a certificate, the KISA shall conduct an identity check in accordance with the procedures for the application for the new issue of a certificate.

It should be noted that the KISA shall conduct identity checks in accordance with the procedures prescribed in its internal regulations for certification practice in the event that a certification authority applies for the suspension or revocation of a certificate using an information communication network.

3.6.2 Certificate Suspension

3.6.2.1 Reasons for Certificate Suspension

If a certification authority applies for the suspension of a certificate, the KISA shall suspend its certificate in accordance with Provision 1 of Article 17 and Provision 2 of Article 25 of the Electronic Signature Law.

3.6.2.2 Applicant for Certificate Suspension

A certification authority can apply for the suspension of its certificates.

3.6.2.3 Submission of an Application for Certificate Suspension

A certification authority can submit an application for certificate suspension by visiting the KISA in person after filling out the necessary items in the application for certificate suspension provided by the KISA, or may submit an application for certificate suspension that has been electronically signed to the KISA using an information communication network.

3.6.2.4 Renewal and Notification of Certificate Revocation List

If a reason for certificate suspension occurs, the Security Agency shall promptly issue the certificate suspension or revocation list for the certificate.

The KISA shall renew the certificate revocation list and promptly announce the fact of its renewal so that it can be easily confirmed by anyone through the certification management system.

3.6.3 Certificate Revival

3.6.3.1 Applicant for Certificate Revival

A certification authority can apply for the revival of its suspended certificates.

3.6.3.2 Submission of an Application for Certificate Revival

A certification authority shall fill out the necessary items in an application for certificate revival that is provided by the KISA, and then submit it to the KISA via direct visit.

3.6.3.3 Notification of Certificate Revival

The KISA shall promptly announce certificate revival, so that the fact can be easily confirmed by anyone through the certification management system.

3.6.3.4 Time Limit for Application for Certificate Revival

A certification authority shall apply for certificate revival within six months from the date of certificate suspension, in accordance with Provision 1 of Article 17 and Provision 2 of Article 25 of the Electronic Signature Law.

3.6.4 Certificate Revocation

3.6.4.1 Reasons for Certificate Revocation

The KISA shall revoke a certification authority's certificates in accordance with Provision 1 of Article 18, Provision 4 of Article 21, and Provision 2 of Article 25 of the Electronic Signature Law, if any of the following reasons occurs:

- o If a certification authority applies for certificate revocation;
- o If the KISA recognizes that a certification authority has certificates issued in deception or forgery, other through illegal methods;
- o If the KISA recognizes that a certification authority has been dissolved;
- o If the KISA recognizes that a certification authority's electronic signature creation keys have been lost, damaged, stolen or leaked

The KISA shall revoke certificates issued by a certification authority that has been cancelled in accordance with Provision 1 of Article 16 and Provision 2 of Article 25 of the Electronic Signature Law.

If the KISA is notified of a vulnerability in the electronic signature creation keys by a

certification authority, the KISA shall revoke the appropriate certification authority's certificates in accordance with '1.3.4.2 Actions on the Vulnerability in Electronic Signature Creation Keys' of this Certification Practice Statement.

If the KISA is notified of a vulnerability in the electronic signature algorithm by a certification authority, the KISA shall revoke the appropriate certification agency's certificates in accordance with '1.3.4.3 Actions on the Vulnerability in Electronic Signature Algorithm' of this Certification Practice Statement.

3.6.4.2 Applicant for Certificate Revocation

A certification authority can apply for the revocation of its own certificates.

3.6.4.3 Submission of an Application for Certificate Revocation

A certification authority shall fill out all necessary items in an application for certificate revocation provided by the KISA, and then shall submit it to the KISA via direct visit.

3.6.4.4 Renewal of Certificate Revocation List and Notification

If a reason for certificate suspension or revocation occurs, the KISA shall promptly issue certificate suspension or revocation list for the certificate.

The KISA shall renew the certificate revocation list and promptly announce the fact of its renewal so that it can be easily confirmed by anyone through the certification management system.

3.6.4.5 Certificate Revocation Delay Period

The KISA shall not have any delay period for handling certificate revocation. If the legitimacy of a reason for certificate revocation is verified, the KISA shall promptly revoke the appropriate certificate.

3.7 Online Certificate Status Protocol (OCSP)

This is not applicable.

3.8 Other Additional Services

The KISA can provide other additional services, such as time-stamping, etc., if applicable.

3.9 Certificate Profile

The KISA shall issue and announce certificates conforming to the standards for X.509 Version 3 Certificate.

3.10 Certificate Revocation List (CRL) Profile

The KISA shall create and announce a certificate revocation list conforming to the standards for X.509 Version 2 Certificate Revocation List.

In the event of the suspension of certificates, the KISA shall show that an appropriate certificate has been suspended using the field for revocation reason code in the zone for the expansion of certificate revocation list.

3.11 Certificate Profile for OCSP Service

This is not applicable.

3.12 Renewal of Electronic Signature Keys

The KISA shall create new electronic signature keys to issue certificates before the validity period of its certificates has expired.

A certification authority shall create new electronic signature keys to apply for the renewal of certificates before the validity period of its certificates has expired.

3.13 Suspension and Revocation of Certification

This is not applicable.

3.14 Suspension or Cancellation of Certification

This is not applicable.

4. Announcement of Information Related to Certification

4.1 Announcement System

The KISA shall announce the information related to the issue, management, etc. of certificates, so that these can be confirmed by anyone through the certification management system.

4.2 Announcement Method

The KISA shall handle the information related to the issue, management, etc. of certificates, and shall promptly announce the same, so that these can be confirmed by anyone through the certification management system.

The KISA shall renew the certificate revocation list on a weekly basis, and promptly announce the renewed list so that it can be confirmed by anyone through the certification management system.

5. Certification Practice System and Equipment Protection Measures

5.1 Physical Protection Measures

5.1.1 Physical Access Control

The KISA shall protect any site where a certification system, etc. is installed from all physical risks, such as the intrusion of an outsider, illegal access, etc.

The KISA shall install and operate a certification system in a separate restricted area, and shall install the corresponding system inside a security cabinet to enable physical access control.

The KISA shall install and operate a monitoring control system, such as a CCTV camera, a monitoring system, an intrusion detection system, etc., which has a warning function to prepare against any abnormal situation.

The KISA's entry control system shall control access to a restricted area through a multi-level identification that combines an identity check card, a fingerprint identification system and weight detection device, etc.

The KISA shall carry out security practice by posting security guards.

5.1.2 Power Supply

The KISA shall use an uninterruptible power supply to prevent serious damage in the event of sudden power failure.

5.1.3 Flood Control

The KISA shall install a certification system away from the floor to ensure that it is protected in the event of a flood.

5.1.4 Fire Prevention

The KISA shall install a fire detector, a portable fire extinguisher, and automatic

extinguishing equipment, etc. in a certification system laboratory.

5.1.5 Storing Media

The KISA shall control physical access by storing the main storing and recording media in a safe.

5.1.6 Waste Handling

The KISA shall physically destroy documents, diskettes, etc. if necessary.

5.1.7 Long-Distance Backup

The KISA shall physically back up long-distance areas with certificates, certificate revocation list, etc. issued by the KISA, which it shall retain for at least 10 years after the appropriate certificate has expired.

5.2 Procedural Protection Actions

5.2.1 Work Classification by Role

The KISA shall classify certification practice according to role to ensure its security and reliability.

5.2.2 Personnel by Main Work

The creation of keys shall be carried out jointly by at least three persons, and other certification practices shall be carried out jointly by at least two persons.

5.3 Technical Protection Actions

5.3.1 Creation of Electronic Signature Keys

The KISA shall allow only authorized persons create electronic signature keys.

The KISA shall create electronic signature keys in a security module that is protected

from physical intrusion, which is not connected to internal and external information communication networks, and which satisfies a secure key creation system or the technical standards in the Rule on Certification Authorities' Installation and Devices.

5.3.2 Key Size and Hash Value

The KISA shall use the following key size and hash value to use a secure and reliable electronic signature algorithm:

- o KCDSA and RSA: Over 2,048 bits
- o ECDSA: Over 163 bits
- o HAS-160 and SHA-1: Over 160 bits

5.3.3 Device for Storing Electronic Signature Creation Keys

The KISA shall securely store and manage electronic signature creation keys using a security module that satisfies the technical standards in the Rule on Certification Authorities' Installation and Devices, so that the electronic signature creation keys are not lost, damaged, stolen or leaked.

5.3.4 How to Delete and Destroy Electronic Signature Creation Keys

If the KISA's certificate expires, or if its electronic signature creation keys are damaged and/or leaked, the KISA shall completely destroy the corresponding medium for storing the electronic signature creation keys, or shall delete the electronic signature creation keys in accordance with the technical standards provided in the Rule on Certification Authorities' Installation and Devices.

5.3.5 Electronic Signature Creation Keys Use Period

The KISA's electronic signature creation keys and those of a certification authority can be used only for the corresponding certificate validity period.

5.3.6 Computer and Network Security Control

The KISA shall use an intrusion detection system and intrusion interception system to

ensure network security.

5.4 Personnel Security

Among the KISA's personnel who manage electronic signature management system, the chief and security manager of a certification management center shall hold a second-class certificate for security clearance.

5.5 Audit Data

5.5.1 Types of Cases in Audit Data

The KISA shall record the cases occurring in a system (hereinafter called as “certification system”) that supports registration information management, the creation and management of electronic signature keys, the creation and issue of certificates, and time-stamping.

5.5.2 Review and Protection of Audit Data

The KISA shall designate a staff member as an audit manager in accordance with its internal regulations of certification practice, and the designated audit manager shall review and archive audit data.

The audit data of each system shall be managed by an audit manager, and each person who manages a system can read only the audit data of the appropriate practice.

5.5.3 Notification of the Occurrence of Incidents

If a security violation incident occurs, notification of such shall be promptly be given to the person in charge.

5.6 Archiving

5.6.1 Types of Objects for Archiving

The KISA shall record and archive the data related to the following practice:

- o Certification practices, including the issue and management of the certificates held by certification authorities
- o Other practices, including the operation of the KISA's key certification system, etc.

5.6.2 Protection of Archives

The KISA shall designate a staff member as a data manager in accordance with its internal regulations of certification practice, and the designated data manager shall manage all archives, while other managers can search only the archives within their work scope.

To prevent archives from being forged and/or damaged, the KISA shall protect archives as follows:

- o Securely retaining electronic data after it has been electronically signed
- o Keeping general documents in a cabinet that has a lock mounted

5.7 Recovery from Glitches and Disasters

5.7.1 Countermeasures in the event of the Occurrence of Glitches in System Sources and Software

If a glitch occurs in a system source, software, etc., the KISA shall recover the same by using double-installed system sources and software.

5.7.2 Countermeasures in the event of Damaged and/or Destroyed Data

If main data such as certification authorities' certificates are damaged or destroyed, the KISA shall recover the same using archived data.

6. Miscellaneous Provisions, Including Certification Practice Guarantee

6.1 Guarantee

6.1.1 Liability for Guarantee

The KISA shall guarantee the following in connection with the certificates that it issues:

- o The accuracy of the contents of an issued certificate
- o The fact that certificates have been issued in accordance with the provisions of the Electronic Signature Law
- o The accuracy of the details of Certificate Revocation

6.1.2 Exemptions

The KISA shall not be liable for any damage caused by reasons not prescribed in the Electronic Signature Law, its enforcement ordinances and regulations or each provision of this Certification Practice Statement, or any damage caused by the delay or impossibility of certification practice treatment due to reasons beyond human control, such as wars, natural disasters, etc.

6.2 Dispute Resolution

6.2.1 Observance Laws

This Certification Practice Statement shall be interpreted and applied in accordance with the Republic of Korea's Electronic Signature Law and relevant laws.

6.2.2 Jurisdiction

The Seoul Central District Court shall be designated as the competent court for the resolution of disputes related to certification practice between the KISA and a certification authority or relying party.

6.2.3 Dispute Mediation

If a dispute occurs between the KISA and a certification authority or a relying party, upon the request of the disputing party, the Minister of Public Administration Security can require the KISA and the certification authority to submit relevant data, induce the parties to mutual agreement via the presentation of a mediation plan after investigating whether the Electronic Signature Law and Certification Practice Statement have been observed, and demand the taking of corrective action.

6.3 Private Information Protection

A top-level certification authority shall conform to the regulations on private information in the Act on Promotion of Information and Communications Network Utilization and Information Protection for the protection of the private information related to the performance of certification practice.

6.4 Audit and Check

6.4.1 Security Check

The KISA shall periodically conduct self-inspections to ensure effective security management when carrying out the certification management center practice, and can request the National Intelligence Service to guide it in security management when changing its system.

6.4.2 Observance of Security Practice Regulations

「A Guide to Security Management in Electronic Signature Certification Management Practice」 shall apply to countermeasures on security that are not stated in this Certification Practice Statement, when the KISA carries out the certification management center practice.

6.5 Observance of Relevant Laws

The KISA's electronic signature certification practice shall conform to this Certification Practice Statement however, the provisions of the Electronic Signature Law, its enforcement ordinances and regulations shall take precedence.

In accordance with copyright laws and other relevant laws, the intellectual property rights of the following shall belong to the KISA:

- o Software and hardware developed by the KISA
- o The KISA's Certification Practice Statement
- o The KISA's names
 - Corporations' names
 - Internet domain names
- o Electronic signature keys, etc. created by the KISA

6.6 Validity of Certification Practice Statement

The established and revised certification practice statement shall [become effective 15 days after the date of its reporting to the Minister of Public Administration and Security.](#)