Certification Practice Statement

Ver 1.1

2001. 11

Korea Information Security Agency

Table of Contents

1. Overview

1.1 Background and Purpose

Digital Signature Act(Law 5792) was established on 5th of February 1999 and has enforced since 1st of July 1999 on the purpose of stimulating national informationalization and increasing the citizen's convenience by defining the basics of establishment and operation of the public key infrastructure and digital signature certification practice structure in order to guarantee safety and trustworthiness of electronic messages in an open network such as the Internet and utilize this.

Certification Practice Statement of Korea Information Security Agency (thereinafter 'KISA') is established to define the necessities relevant to digital signature certification such as certificate policy, issue & practice of certificate, security control and operational policy & procedure and the matters relevant to obligations and responsibilities of KISA and Licensed Certification Authority(thereinafter 'LCA') according to Digital Signature Act, Digital Signature Ordinance(thereinafter `the Ordinance') and Digital Signature Regulations(thereinafter 'the Regulations').

1.2 Scope

Concerning the KISA's digital signature certification practice, provisions of Certification Practice Statement has priority unless the provisions of Digital Signature Act, the Ordinance and the Regulations have been shown.

1.3 Certificate Policy

KISA issues certificates to the LCA, which is nominated under Sec. 4 of the Digital Signature Act, under Sec. 15 and Sub-Sec. 2 of Sec. 25 and suspends or revokes them under Sec. 16, Sec. 18 or Sub-sec. 2 of Sec.25.

1.4 Introduction of Korea Information Security Agency

KISA has its establishment basis provision under Sub-Sec. 1 of Sec. 52 of the Information and Communication Promotion and Information Security Act. KISA is aiming for promoting the national informationalization and facilitating citizen's life by playing a role as a Root Certificate Agency (thereinafter 'RCA') within the digital signature certification practice structure under provisions of Sec. 8 and 25 of the Digital Signature Act, and developing the necessary policy and techniques for establishing

order and distribution of information.

1.4.1 Contact Details

KISA's contact details are as follows:

o URL : http://www.rootca.or.kr
o E-Mail : admin@rootca.or.kr
o Address : KISA, 4th FL., IT Venture Tower, 78, Garak-Dong, Songpa-Gu, Seoul, Korea
o Phone : +82-2-4055-411

1.4.2 Repositories

KISA's repositories are as follows:
o KISA's Certification Practice Statement : http://www.rootca.or.kr/rca/cps.htm
o LCA List : http://www.rootca.or.kr/lca/lca.htm
o Certificate List : http://www.rootca.or.kr/cert.htm
o Certificate Suspension and Revocation List : http://www.rootca.or.kr/crl.htm

1.5 Community

1.5.1 Information Security Promotion Subcommittee

o Deliberation of policy of establishing and running the national public key infrastructure
o Deliberationof building an inter-national mutual certification structure

1.5.2 National Intelligence Service

o Deliberation of whether the real inspection result of nomination of an LCA for a governmental and municipal authority is in accord with national security policy
o Security guidance for KISA's certification practice
o Security guidance for certificationpractices of the LCAwhen a governmental or municipal authority is nominated as an LCA

1.5.3 Ministry of Information and Communication

Ministry of Information and Communication works as a policy maker and inspector for a secure operation of digital signature certification practice structure as described below:

- o Policy making for securely establishing and running the digital signature certification practice structure
- o Nomination, correcting order, suspension of a practice, cancellation of the nomination and investigation of LCAs
- o Managing and inspecting the KISA and LCA's compliance with the Digital Signature Act, the Ordinance and the Regulations
- o Mutual accreditation of digital signature with a foreign government

1.5.4 Korea Information Security Agency

KISA plays a role, under Sec. 8, 10, 12 and 25 of the Digital Signature Act in order to fulfill its responsibilities in the digital signature certification practice structure as a RCA as below:

- o Establishing and running the secure digital signature certification practice structure
- o Certification practices such as certification for public key of an LCA
- o Taking over the subscriber's certificate of the LCA whose certification practice is revoked
- o Taking over the subscriber's certificate of the LCA whose nomination iscancelled
- o Establishing and running a mutual certification structure
- o Developing and distributing a digital signature certification technique
- o Real investigation to nominate an LCA
- o Inspecting an LCA and supporting a secure operation
- o Time-stamping service
- o Other digital signature certification related practices

1.5.5 Licensed Certification Authority

LCA provides a public certification practice to subscribers as a governmental authority, as a municipal authority or as a corporation nominated by the provisions of Sec. 4 of the Digital Signature Act. However, a party who is under the reason of disqualification in Sec. 5 of the Digital Signature Act cannot be nominated as an LCA.

- o Identification
- o Certificate issuance

o Certificate suspension and revocation
o Certificate renewal
o Notification of certificate-related information
o Time-stamping practice

1.5.6 Relying Party

Relying Party trusts and uses the certificate issued by KISA. See below:

o LCA
o LCA subscribers
o Mutually authenticated foreign LCA under mutual certification
o Mutually authenticated foreign LCA subscriber under mutual certification

1.6 Applicability

The certificate signed and issued by KISA is used for proving that public key is in accord with the KISA's private key.

The certificate issued to an LCA by KISA is used for proving that public key of an LCA is in accord with its private key.

KISA can issue the certificate which limits the utilization range and use under Sub-Sec. 4 of Sec. 15 and Sub-Sec. 2 of Sec. 25 when an LCA applies for.

1.7 Person determining CPS suitability for the Policy

The Director of KISA has a right of establishment and revision of Certification Practice Statement. The establishment and revision must be reported to the Minister of Information and Communication under Sub-Sec. 1 of Sec. 6 and Sub-Sec. 2 of Sec. 25 of the Digital Signature Act.

2. General Provisions

2.1 Obligations

2.1.1 Korean Information Security Agency Obligations

2.1.1.1 Providing and Notifying Accurate Information

KISA immediately notifies the LCAs and the relying parties of the information as below which can affect the trustworthiness or validity of a certificate in order to help anybody confirming it under the certification practice structure.

o Information on an LCA
  - LCA nomination
  - Suspension or revocation of an LCA certification practice
  - Cancellation of an LCA nomination
  - Transfer or merger of an LCA
o Information about certificate
  - Certificate
  - Certificate suspension and revocation list
o Other certification practice related information

2.1.1.2 Providing a Directory Service

KISA provides the directory management enabling LCA and the relying party to search KISA's certificates, LCA's certificates, suspension and revocation list of certificates through information and communication networks.

2.1.1.3 Measures on Vulnerability of Private Key

KISA revokes the KISA's certificate including public key in accord with private key and reissues the KISA's certificate by creating a new key pair when KISA recognizes that its private key is not secure. After renewal and issuance of an LCA's certificate using a new private key, KISA immediately notifies the matters that everybody can identify and take measures to guarantee the safety and trustworthiness in the management under the certification practice structure.

KISA, when informed of the loss and damage, theft, drain or vulnerability about the

private key from an LCA, revokes the certificate issued to the LCA and notifies the matters everybody can identify under the certification practice structure. KISA, when being informed of loss and damage or theft, drain and vulnerability from the LCA of a governmental and municipal authority, immediately inform it to the Director of the National Intelligence Service.

2.1.1.4 Measures on Vulnerability of Digital Signature Algorithm

KISA, when recognizing that its digital signature algorithm is not secure, revokes the KISA's and LCA's certificates issued by using its digital signature algorithm as well as immediately notifies the matters everybody can identify and takes measures to guarantee safety and trustworthiness in the practice under the certification practice structure.

KISA, when informed vulnerability about the sigital signature algorithm from an LCA, revokes the certificate issued to the LCA and notifies the matters everybody can identify under the certification practice structure. KISA, when informed vulnerability about the digital signature algorithm from the LCA of a governmental and municipal authority, immediately informs it to the Director of the National Intelligence Service.

2.1.2 Licensed Certification Authority Obligations

2.1.2.1 Providing and Notifying Accurate Information

An LCA has to provide accurate information and facts to KISA in the cases below.

- o Real investigation relevant to an LCA nomination
- o Certificate issuance application
- o Application for a certification suspension and revocation
- o Certificate reinstatement application

LCA has to notify the subscribers and the relying parties of the information as below which can affect the trustworthiness or validity of a certificate in order to help anybody confirming it within the certification practice structure.

- o LCA notification
- o Certification suspension and revocation practice of an LCA
- o Cancellation of LCA nomination

o Transfer or merger of an LCA
o Information on a certificate
  - Subscriber's certificate
  - Certification suspension and revocation practice of a subscriber
o Other certification practice related information

2.1.2.2 Protecting Private Key

LCA must create its own key pair in a secure way using a trustworthy software or hardware and manage its private key securely not to be lost, damaged, stolen or drained.

When creating a subscriber's key pair, LCA must create in a secure way using a trustworthy software or hardware and distribute the private key securely not to be lost, damaged, stolen or drained.

2.1.2.3 Using a Certified Private Key

LCA has to use the private key in accord with a KISA-certified public key when providing a certification practice.

2.1.2.4 Notification and Measures about Loss and Damage or Theft or Drain of Private Key

LCA, when its private key is lost, damaged, stolen or drained, takes measures to guarantee safety and trustworthiness by reporting to KISA under Sub-Sec. 3 of Sec.21 of the Digital Signature Act.

2.1.2.5 Notification and Measures about Vulnerability of Private Key

When recognizing its private key is not secure, LCA immediately reports it to KISA and takes measures to guarantee safety and trustworthiness.

2.1.2.6 Notification and Measures about Vulnerability of Digital Signature Algorithm

When recognizing its digital signature algorithm is not secure, LCA immediately reports it to KISA and takes measures to guarantee safety and trustworthiness.

2.1.3 Relying Party Obligations

2.1.3.1 Understanding of Purpose in Use of Certificate

Relying party has to understand the purpose in use of certificate issued by KISA under the Certification Practice Statement '1.6 Certificate Usage Range and Use'.

2.1.3.2 Confirming Certificate

Relying party has to verify the certificate's valid period, utilization range, use and trustworthiness prior to using the certificate.

2.1.3.3 Confirming Suspension and Revocation of Certificate

Relying party has to verify and confirm the validity of a certificate through the certificate suspension and revocation list prior to using the certificate.

2.2 Liability of Korea Information Security Agency

2.2.1 Liability of Warranties

KISA guarantees the below relevant to the certificate issued by itself.

- o The contents in the issued certificate are correct.
- o The certificate is issued under the Digital Signature Act.
- o The matters about suspension and revocation of certificate are correct.

2.2.2 Exemption from Liability

KISA has no responsibility for any delays in certification practice or damages due to force majeures such as warfare and a natural disaster or reasons beyond provisions of the Digital Signature Act, the Ordinance and the Regulations.

2.3 Interpretation and Enforcement

2.3.1 Applicable Law

The Certification Practice Statement is interpreted and applied under the Digital Signature Act and relevant regulations.

2.3.2 Competent Court

Seoul District Court is the competent court to mediate a dispute relating to certification practices between KISA and an LCA or a relying party.

2.3.3 Dispute Resolution

Minister of Information and Communication can order a corrective action at the same time with guiding them to mutual consent by suggesting a mediation plan through requesting related materials to KISA and to an LCA and investigating the observance of the Digital Signature Act and the Certification Practice Statement.

2.4 Fees

2.4.1 Fee for Issue, Reissuance and Renewal of Certificate

KISA may make a charge to the LCA applying for issue, reissuance or renewal of certificate observing fee estimation standard defined by the president of KISA.

2.4.2 Certificate Access Fee

KISA makes no charge to the relying party reading and confirming certificates.

2.4.3 Access Fee for Suspension and Revocation List of Certificate

KISA makes no charge to the relying party accessing the suspension and revocation list of certificates.

2.4.4 Fees for Other Service

KISA can make charge for the other practices if needed under the provisions of the Digital Signature Act.

2.5 Notification

2.5.1 Korea Information Security Agency's Notification

KISA notifies information relevant to the issue and practice of certificate in order to help anybody confirming it under the certification practice structure.

2.5.2 Notification Frequency

KISA immediately notifies after processing the information relevant to the issue and practice of certificates in order to help anybody confirming it under the certification practice structure.
KISA immediately notifies after renewing the suspension and revocation of certificates once in a week in order to help anybody confirming it under the certification practice structure.

2.6 Intellectual Property Rights

Intellectual property rights listed in below belong to KISA according to the Copyright Act and other related regulations:

- o Software and hardware developed by KISA
- o Certification Practice Statement of KISA
- o the Name of KISA
  - Corporate Name
  - Internet Domain Name
- o Key pair created by KISA

3. Identification

3.1 Identification at New Certificate Application

3.1.1 Uniqueness of Names

The names used in basic area of a certificate, suspension of a certificate and an revocation list apply X.500 DN(Distinguished Name).
DN in the certificate issued by KISA uses an authority name or a corporate name.

3.1.2 Authentication of Organization Identity

KISA confirms an LCA through a designation letter and a certified copy of registration of the LCA and through equivalent documents of government and municipal authorities.

3.1.3 Authentication of Individual Identity

KISA identifies a certificate applicant or a application agent through an interview in following way:

o Identifying the real name of the applicant by checking an identification card or a passport, the certificate issued by the government

o Identifying the certificate applicant or the application agent by the documents proves that he/she is an employee belonging to an LCA and confirming whether the applicant is in his/her capacity as a representative or the agent has the right of representation of the applicant.

3.2 Identification at Certificate Reissuance

When an LCA applies for a reissuance of a certificate due to the expiration of the term or revocation of the certificate, KISA identifies with a procedure corresponding to the application for a new issue.

3.3 Identification at Certificate Renewal

When an LCA applies for a renewal of a certificate in order to change information except public key and DN included in its certificate, KISA identifies the LCA in procedure corresponding to the application for a new issue.

3.4 Identification at Certificate Suspension and Revocation Application

When a representative of an LCA or his/her agent applies for a suspension and revocation of a certificate through visitation, KISA identifies him/her in procedure corresponding to the application for a new issue.

When an LCA applies for suspension and revocation of a certificate through an information and communication network, KISA identifies according to the procedure defined by its certification practice internal regulations.

3.5 Identification at Certificate Reinstatement

When an LCA applies for reinstatement of a certificate, KISA identifies according to procedure corresponding to the application for a new issue.

4. Operational Requirements

4.1 Certificate Application

An LCA applies for a certificate through visitation after filling out an application form. The form and relevant information can be obtained directly from the KISA office or downloaded from the KISA's official web site.

4.2 Certificate Issuance

4.2.1 New Certificate Issuance

KISA issues the certificate after checking the following criteria prior to the new issue of the certificate.

- o Identification according to the Certification Practice Statement '3.1 Identification at New Certificate Application'
- o Uniqueness of the public key submitted by a certificate applicant
- o Whether the public key submitted by a certificate applicant is in accord with the private key owned by its LCA
- o Uniqueness of DN submitted by a certificate applicant

4.2.2 Certificate Reissuance

KISA reissues the certificate after checking the following criteria prior to the reissuance of the certificate.

- o Identification according to the Certification Practice Statement '3.2 Identification When applying for a Certificate Reissuance'
- o Uniqueness of the public key submitted by a certificate applicant
- o Whether the public key submitted by a certificate applicant is in accord with the private key owned by its LCA
- o Uniqueness of DN submitted by a certificate applicant

4.2.3 Certificate Renewal

KISA renews the certificate after checking the following criteria prior to the renewal of the certificate.

o Identification according to the Certification Practice Statement '3.3 Identification When applying for a Certificate Renewal
o Conformity between the public key submitted by a certificate applicant and the public key listed in the previous certificate
o Conformity between the DN submitted by a certificate applicant and the DN listed in the previous certificate

4.2.4 Information in Certificate

The certificate issued by KISA includes the followings under provisions of Sub-Sec. 2 of Sec. 15 and Sub-Sec. 2 of Sec. 25 of the Digital Signature Act

o Name of the LCA
o Public key of the LCA
o KISA and a LCA's digital signature methods
o Serial number of the certificate
o Valid term of the certificate
o Name of KISA as a RCA
o Details of limiting the utilization range and use of the certificate, etc.

4.2.5 Valid Period of a Certificate

KISA sets the valid term of a certificate considering its utilization range, use, safety and trustworthiness of the applied technology under the provisions of Sub-Sec. 5 of Sec. 15 and Sub-Sec. 2 of Sec. 25.

o Valid term of a certificate of KISA must be within 10 years.
o Valid term of an LCA's certificate issued by KISA must be within 5 years.

4.2.6 Acceptance of a Certificate

An LCA must collect the certificate through visitation within 48 hours from the notification of the collection. KISA revokes it if the LCA does not collect the certificate within 48 hours.

The LCA can use the certificate from the start date of the valid term.

4.3 Certificate Suspension

4.3.1 Circumstances for Suspension

When an LCA applies for suspension of the certificate, KISA suspenses the validity of the certificate.

4.3.2 Who Can Request Suspension

An LCA can apply for the suspension of its own certificate.

4.3.3 Procedure for Suspension Request

4.3.3.1 Submitting a Certificate Suspension Request Form

An LCA can submit a certificate suspension request form to KISA directly through visitation or the digitally signed certificate suspension request form through an information and communication network.

4.3.3.2 Identification

KISA proves its identity according to the Certification Practice Statement '3.4 Identification at Suspension and Certificate Revocation

4.3.3.3 Renewal and Notification of a Certificate Suspension and Revocation List

KISA renews the certificate suspension and revocation list and immediately notifies in order to help anybody confirming it under the certification practice structure.

4.3.4 Renewal Frequency of Certificate Suspension and Revocation List

When the reasons of suspension and revocation of a certificate occur, KISA immediately issues a certificate suspension and revocation list for the certificate.

KISA renews the certificate suspension and revocation list once a week.

4.4 Certificate Reinstatement

4.4.1 Who Can Request Reinstatement

LCA can apply for the reinstatement of the suspended certificate.

4.4.2 Procedure for Reinstatement

4.4.2.1 Submitting a Certificate Reinstatement Request Form

An LCA submits a certificate reinstatement request form to KISA directly through visitation.

4.4.2.2 Identification

KISA proves its identity according to the Certification Practice Statement '3.5 Identification at Certificate Reinstatement.'

4.4.2.3 Notification of a Certificate Reinstatement and Revocation List

KISA updates the certificate reinstatement and revocation list and immediately notifies in order to help anybody confirming it under the certification practice structure.

4.4.3 Limits on Suspension Period for Reinstatement

An LCA must apply for the reinstatement of a certificate within 6 months since its suspension date under the provisions of Sub-Sec. 1 of Sec. 17 and Sub-Sec. 2 of Sec. 25 of the Digital Signature Act.

4.5 Certificate Revocation

4.5.1 Circumstances for Revocation

According to the provisions of Sub-Sec. 1 of Sec. 18, Sub-Sec. 4 of Sec. 21 and Sub-Sec. 2 of Sec. 25 of the Digital Signature Act, KISA revokes a certificate of an LCA in the cases below:

- o When an LCA applies for a certificate revocation
- o When the KISA recognizes that a certificate of an LCA was issued in the illegal manner, such as fraud or forgery

o When the KISA recognizes the dissolution of an LCA
o When the KISA recognizes that a private key of an LCA is lost, damaged, stolen or drained

KISA revokes the nomination-cancelled certificate of an LCA under the provisions of Sub-Sec. 1 of Sec. 16 and Sub-Sec. 2 of Sec. 25 of the Digital Signature Act. According to the Certification Practice Statement '2.1.1.3 Measures on Vulnerability of Private Key', KISA revokes the certificate of the LCA when informed the vulnerability of the private key.

According to the Certification Practice Statement `2.1.1.4 Measures on Vulnerability of Digital Signature Algorithm', KISA revokes the certificate of the LCA when informed the vulnerability of the digital signature algorithm.

4.5.2 Who Can Request Revocation

An LCA can apply for the revocation of its certificate.

4.5.3 Procedure for Revocation Request

4.5.3.1 Submitting a Certificate Revocation Request Form

An LCA can submit a certificate revocation request form to KISA directly through visitation or the digitally signed certificate revocation request form through an information and communication network.

4.5.3.2 Identification

KISA proves its identity according to the Certification Practice Statement '3.4 Identification When applying for Suspension and Certificate Revocation.'

4.5.3.3 Renewal and Notification of a Certificate Suspension and Revocation List

KISA renews the certificate suspension and revocation list and immediately notifies in order to help anybody confirming it under the certification practice structure.

4.5.4 Grace Period for Certificate Revocation

KISA has no grace period for certificate revocation and revokes the certificate as soon

as it confirms the legitimacy of the certificate revocation.

4.5.5 Renewal Frequency of Certificate Suspension and Revocation List

KISA updates the certificate suspension and revocation list and immediately notifies in order to help anybody confirming it under the certification practice structure.
KISA renews the certificate suspension and revocation list once a week.

4.6 Security Audit Procedure

4.6.1 Type s of Event Recorded

KISA records the followings on the audit log file created in the key creation system, certificate issue & practice system, directory system and time-stamping system(hereinafter 'Main Certification Systems').

- o Statement about entry, access, change and deletion of subscriber's property, the time, and the transactor
- o Statement about creation, access and destruction of a key pair, the time, and the transactor
- o Statement about creation, issuance, renewal, suspension and revocation of a certificate, the time, and the transactor
- o Statement about registration and practice of subscribers' certificates, the time, and the transactor
- o Statement about time-stamping of an electronic message, the time, and the transactor
- o Statement about start and close of the main certification system, the time, and the transactor
- o Statement about login and log-off, the time, and the transactor
- o Statement about main activities of the main certification system administrator, the time, and the transactor

4.6.2 Review and Protection of Audit Log

The audit administrator overall manages the audit log of each systems. And the other administrators in each system can read the relevant audit log.

4.6.3 Event Occurrence Report

Report to a relevant administrator through auto-alarm of the intrusion detection system in case of the security violation.

4.6.4 Vulnerability Assessment

KISA regularly takes self- vulnerability assessment in order to provide an efficient security control measure against the change of the operational environment and threat.

4.7 Record Archival

4.7.1 Types of Event Archived

KISA logs and archives the practices related to below:

- o Service of real investigation for nomination of an LCA
- o Service for issue and practice of a certificate of an LCA
- o Service for running the main certification system of KISA

4.7.2 Protection of the Archived Record

KISA preserves the logs as below in order to prevent the forgery, alteration and damage of the records.

- o An electronic message must be securely stored with digital signature.
- o A normal message must be stored in a cabinet with a lock.

4.8 Key Changeover

When necessary to reissue a certificate due to the expired valid term, KISA issues a certificate through issuing a new key pair prior to the expiration date.

When needed to reissue a certificate due to the expired valid term, an LCA has to apply for issuing a certificate through issuing a new key pair prior to the expiration date.

4.9 Recovery Measures

4.9.1 Measures for System Resources and Software Malfunction

When there are malfunctions in the system resources and software, KISA recovers it by duplicated system resources and software.

4.9.2 Measures for Data Corruption

When there are damage and loss of important data such as a certificate from an LCA, KISA recovers it by the logs and archived data.

5. Physical, Procedural and Personnel Security Controls

5.1 Physical Control

5.1.1 Physical Access Control

KISA protects the place equipped with the main certification system from a physical threat such as an intrusion or an illegal access.

- o Establishing and running the main certification system of KISA in a restricted area
- o The entrance control system controls access to the restricted area through mixture of the ID card, the fingerprint recognition and the weight detection
- o Installing the main certification system of KISA in the security cabinet to restrict the physical access.
- o When an external personnel enters the main certification system, the manager in charge of that area must be accompanied.
- o KISA records the access to the restricted area and regularly examines the record.
- o KISA installs and operates the surveillance control system with an alarm for abnormal situation.
  - CCTV camera and monitoring system
  - Intrusion detection system
- o KISA has to arrange 2 security guards.

5.1.2 Power Supply

KISA has to use UPS(Uninterrupted Power Supply) to avoid a fatal damage resulting from a power failure.

5.1.3 Prevention of Flood

KISA installs the main certification system at least 30 cm above the ground to protect the system from an inundation.

5.1.4 Fire Prevention

KISA installs a fire sensor in rooms such as the main certification system room.

KISA installs extinguishing equipments such as a fire extinguisher in the main

certification system room.

5.1.5 Media Storage

KISA controls access physically by keeping the storage and recording media in a safe.

5.1.6 Waste Disposal

KISA destroys documents, diskettes and so on physically.

5.1.7 Off-Site Backup

KISA keeps certificates, certificate suspension and revocation lists, which are issued by KISA, for 10 years from its suspension by backup in a physical remote place.

5.2 Procedural Control

5.2.1 Functional Service

KISA performs its practice separately according to the practice function to guarantee the safety and trustworthiness.

5.2.2 Minimum Number for Services

Key generation service team consists of at least 3 persons.

Other certification practice team consists of at least 2 persons.

5.3 Personnel Control

Director and security operator in Korea Certification Authority Central working forces in KISA must have a second-rate secret license.

5.4 Security Control

KISA regularly have a self-inspection for efficient security control in the Certification Practice Center practice and can request a security guidance to the

National Intelligence Service more than once a year.

5.5 Compliance with Security Service Regulations

KISA observes 'Security Service Regulations' for the security measures which are not shown in the Certification Practice Statement in the Certification Practice Center practice.

6. Technical Security Controls

6.1 Key Pair Generation

6.1.1 Key Pair Generation

KISA allows the authorized personnel to create a key pair.

KISA creates the key pair in a secure key generation system which is not connected to internal and external network as well as is protected from physical infringement.

6.1.2 Key Size and Hash Value

KISA uses the following keys and hash values to have a secure and trustworthy digital signature algorithm.

- o KCDSA and RSA : 2,048 bit or more
- o HAS-160 and SHA-1 : 160 bit or more

6.2 Private Key Protection

6.2.1 Private Key Storage Device

KISA stores the private key with double encryption in a storage equipped with sealing, access authority confirmation and anti-drain & alteration of key pair functions.

6.2.2 Secure Clearing after Private Key Usage

KISA deletes the private key from a system memory as soon as finishing the creation and use of the private key.

6.2.3 Private Key Termination

KISA destroys the storage media for the private key physically and completely when the effective terms of the certificate is expired or the private key is damaged or released out.

6.3 Valid Term of Private Key

KISA and an LCA's private key can be used while the certificate is valid.

6.4 Computer and Network Security Control

KISA uses the intrusion detection system in order to prevent the counter-service attack.

KISA uses the intrusion detection system with an evaluation certificate in order to protect.

7. Certificate, Certificate Suspension and Revocation List Profile

7.1 Certificate Profile

KISA issues and notifies the certificate applying with X.509 version 3 certificate standard.

7.2 Certificate Suspension and Revocation List Profile

KISA issues and notifies the certificate suspension and revocation list applying with X.509 version 2 certificate revocation list standard.

KISA indicates the suspended certificate using a revocation reason code field from an extension area of the certificate suspension and revocation list when suspended the certificate.

8. Certification Practice Statement Administration

8.1 Revision Procedure

When the Minister of Information and Communication orders an alteration of the Certification Practice Statement, KISA revises the rule.

When the Director of KISA decides an alteration of the Certification Practice Statement, KISA revises the rule.

KISA maintains the revision-related record of the Certification Practice Statement including the belows:

- o Version of the Certification Practice Statement
- o Overview of the applied practice and range
- o Revision record of the Certification Practice Statement
  - Previous provisions of the Certification Practice Statement
  - Revised contents
  - Reason of the revision

8.2 Enforcement Procedure

KISA reports the established and revised Certification Practice Statement to the Minister of Information and Communication.

KISA notifies the established and revised Certification Practice Statement on the Certification Practice Statement '1.4.2 Repositories' and individually informs it to the LCAs.

The established and revised Certification Practice Statement is in force since the day of report.

Glossary

o DN(Distinguished Name)

Name which applies with X.500 standard using for identifying the certificate issuer and the certificate holder.

o Subscriber

Who has a certificate for his/her digital signature verification key from an LCA.

o LCA

Who provides a public certification service designated by the Minister of Information and Communication under Sec. 4 of the Digital Signature Act.

o Directory

Which keeps certificates, certificate suspension and revocation list, and provides notification and search services to a relying party. It applies with X.500 standard.

o Denial of Service Attack

Offensive activity to obstruct the normal operation of the system.

o Relying Party

A party who trusts and uses the certificate obtained from KISA.

o Identification

Activities that confirm the LCA, the applicant and authenticity of application information to guarantee the trustworthiness of the certificate when applying for issuance, renewal, suspension and revocation of certificate.

o Real Name

The name in the social security card, the name in the certificate of inscription for

business, or the real name under the law for financial transaction with real name and protection of security information and its ordinance(Presidential decree 15744).

o Certification

Activity which confirms and verifies that the public key has conformity with the private key owned by a natural person or a legal entity.

o Certification Practice Structure

A system under which certification services, such as the issuance of certificates and maintenance of certification-related records, are performed.

o Certificate

Information in electronic form verifying and certifying the correspondence of a public key to a private key owned by a natural person or legal entity.

o Certification Practice

The practices employed in providing certification services such as the issuance of certificates and the maintenance of certification-related records.

o Electronic Message

Information generated, communicated, received, or stored in an electronic form by a device possessing data processing capabilities such as a computer.

o Digital Signature

Digital signature means information, which is unique to an electronic message, created by a private key using an asymmetric crypto-system such that the identity of the person generating the electronic message and any possible alteration thereof can be verified.

o Public Key

Electronic information to verify the digital signature.

o Private Key

Electronic information to generate the digital signature.

o Key pair

It means both private key and its corresponding public key.

o Main Certification System

It means key generating system, certificate issuance & practice system, directory system and time-stamping system.