Certification Practice Statement
Version 2.2

1. Introduction

1.1 Background and Objective

1.1.1 Background and Objective of Practice Statement

The Digital Signature Act (Law No. 5,792) was enacted on February 5, 1999 and implemented from July 1, 1999 for the purpose of stimulating the informatization of Korea and promoting the convenience of its people by determining the basic matters on digital signatures, in order to utilize the security and reliability of digital documents that use and process open information and communication systems (such as the Internet).

The Certification Practice Statement of Accredited Certification Center of SignKorea (English name: SignKorea, hereinafter referred to as “SignKorea”) aims to specify the regulation on Responsibility and Obligation related to the Accredited Certification service and the comprehensive matters required in accredited certificate works (hereinafter referred to as "Accredited Certification Service") such as issuance, suspension, reinstatement, renewal, revocation and others of accredited certificate provided by SignKorea under its design as the accredited certificate institution.

1.1.2 Digital Signature Certification Scheme: Introduction

“Digital Signature Certification Scheme” (hereinafter referred to as “Certification Scheme”) refers to the scheme that provides issuance of accredited certificate, administration of certification-related records and other relevant works using the accredited certificate.

1.1.3 Accredited Certification Authority: Introduction

SignKorea was established in July of 1999 for the purpose of building up an exchange environment for safe digital documents by using the digital signature method within information and communication environments pursuant to the Digital Signature Related Act.

The accredited certificate center of “SignKorea” was designated as an accredited certificate institution (Designation Number 2) by the government on February 10, 2000 pursuant to Article 4 (Designation of Accredited Certification Authority).

The following are the places and points of contact for SignKorea in relation to the accredited certification service.

○ Name of Institution: Accredited Certification Center of SignKorea (English name: SignKorea)
○ Address
- Head office : 33 Yeouido-dong, Yeungdeungpo-gu, Seoul, Korea (150-010)
- SignKorea : 246-4 Seohyeon-dong, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea (463-824)
- SignKorea Anyang: 1026-7, Hogye-dong, Dongan-gu, Anyang-si, Gyeonggi-do, Korea (431-848)

○ Internet URL: http://www.signkorea.com
○ E-mail: signkorea@signkorea.com
○ Telephone: 1577-7337
○ Fax: 02) 767-7390

1.1.4 Accredited Certificate: Definition and Effect

"Accredited Certificate" refers to the accredited certificate that SignKorea issues to the party that wishs to issue it pursuant to Article 15 (Issuance of Accredited Certification) of the Digital Signature Act. In this case, SignKorea shall verify the identification of the party that intends to use the accredited certificate.

The accredited digital signature on the accredited certificate issued by SignKorea is assumed to be either the signature or affixing of seal of the signer and is considered that the content of the digital document has remained unchanged after the digital signature was made. In addition, it shall be effective as the signature or affixing of seal in accordance with the agreement between the concerned parties.

SignKorea issues the certificate that has an digital signature generated with the generation key of the certification authority, for the relevant information with the verification key that a subscriber has submitted after confirming the consistency of the information as provided by the subscriber at the time of subscribing. Therefore, SignKorea guarantees to users that the details listed on the certificate of SignKorea shall be genuine fact at the time of applying for the issuance of the certificate, but not the guarantee of the following.

○ Guarantee on specific work or purpose of subscriber and user
○ Credibility of subscriber
○ Invariability of information related to the identity of subscriber identification and others
○ Other field of works for SignKorea

In the event that a subscriber generates the digital signature with the generation key that is consistent to the verification key of the certification, the generated digital signature is deemed as the signature or affixing of seal on the applicable document pursuant to Article 3 (Validity of Digital Signature) of the Digital Signature Act.

Certification of SignKorea may be used in fields where legal rights and obligations arise including the generation of digital signature and verification of digital document exchange, software verification and others as well as the personal identification field on the other party under the situation where the parties do not interact face to face.

SignKorea does not determine separate use as prohibited scope, however, pursuant to Article 16 (Validity of Certification) of the Digital Signature Act, the use of certificate of a subscriber may be limited in the following cases.

○ In the event the identification or legitimate e-commerce is impossible due to the death, arrest and others of subscriber

○ In the event the subscription is made by an incompetent person or quasi-competent person without going through the legal agent

○ In the event the subscription is made by an incompetent person or quasi-competent person without the agreement of the legal agent

○ In the event that the effective period of certificate is lapsed

○ In the event that SignKorea finds out that subscriber was issued with the certificate in an illegitimate method

○ In the event that SignKorea deems it necessary to limit the use of certificate issued for security reasons such as the release of generation key for the certification authority or the security procedure related to the certification service

○ In the event that the applicable certificate is used for the purposes of verification on identity, position of subscriber or certificate to prove the identity

○ In the event that SignKorea may limit the use of certificate

1.2 Name of the Certification Practice Statement

The name of this practice statement is the Certification Practice Statement of SignKorea Ver 2.2.

1.3 Concerned Parties to the Digital Signature Certification Scheme

1.3.1 Ministry of Public Administration and Security

The Ministry of Public Administration and Security is the policy and supervisory institution for the safe and reliable operation of digital signature certification management systems and performs the following.

○ Policy establishment for safe and reliable structuring and operating of the digital signature certification management system

○ Designation, order of correction, work suspension, designation cancellation and investigation of the certificate Authorities

○ Management and supervision on compliance of Digital Signature Related Act by the certificate authorities

○ Mutual recognition of digital signature with foreign governments, etc.

1.3.2 Korea Information Security Agency

The Korea Information Security Agency undertakes the following works for the purpose of carrying out its missions and roles as the highest certification institution in the digital signature certification management system under the provisions of Article 8 (Work Performance of Certification Authority), Article 10 (Discontinuation, Closure of Certification Work), Article 12 (Suspension, and Cancellation of Designation of Certification Work) and Article 25 (Digital Signature Certification Management Work) of the Digital Signature Act.

○ Structure and operation of a safe digital signature certification management system

○ Performing certification work including the certification on the digital signature verification key of the certification authority

○ Acquisition of subscriber certification of the certification authority that closed the certification work

○ Acquisition of subscriber certification that has its designation as a certification institution cancelled

○ Structuring and operating of mutual certification system

○ Development and dispersion of digital signature certification technology

○ Practical inspection for the certification authority designation

○ Support of inspection and safe operation of certification institution

○ Time stamp service

○ Other works related to digital signature certification

1.3.3 SignKorea

SignKorea is the institution designated as a certification institution with the review of government pursuant to Article 4 (Designation of Certification Authority) and Article 8 (Work Performance of Certification Authority) of the Digital Signature Act and carries out the following.

○ Reception and processing of applications related to certification service

○ Identification of subscribers

○ Providing the certificate and related information

○ Providing certification service

○ Providing certificate revocation list (including the validity suspension list)

○ Designation and management of Registration Authority and Local Registration Authority (hereafter referred to as the "Registration Agency")

○ Other works to be performed as the certification authority

1.3.3.1 Responsibility and Obligations

1.3.3.1.1 Providing Accurate Information

SignKorea shall provide only accurate information and facts to the Korea Information Security Agency in relation to the following.

○ Substantive inspection related to the certification authority designation
○ Application to issue (including renewal and re-issuance) certificate for a certification institution
○ Application for suspension of validity and revoke of certificate for a certification institution

SignKorea shall guarantee the following matters to subscribers and users by issuing the certificate for subscriber with the generation key as consistent to the verification key included in the certificate for certifying institution issued by the Korea Information Security Agency.

○ The information in the certificate issued by SignKorea shall have no error.
○ During the course of issuing the certificate, there is no error of information caused by the mistake of SignKorea on the route to SignKorea from the certificate subscriber.

1.3.3.1.2 Providing Certification Service Related Information

SignKorea provides the rules and related information through the homepage determined in 1.4.3 (Notice on Statement and Method of Subscriber Agreement), and registers the information related to the certificate and suspension and revoke of validity on certificate on the directory or web-server system to allow subscribers and users to search at all times.

1.3.3.1.3 Protection of Subscriber Information

SignKorea shall classify the information of subscribers as classified pursuant to Article 24 (Protection of Personal Information) of the Digital Signature Act, and shall limit the unauthorized access of others, and does not permit the unauthorized changes or deletion by others even for the information disclosed with the Agreement of a subscriber. However, SignKorea may disclose the information in the event that the other institutions request pursuant to the provisions under the law or regulation.

1.3.3.1.4 Correct Use of Generation Key

SignKorea may make several pairs of digital signature keys for the use purposes as below. However, each pair of digital signature key is usable only in the applicable field.

◯ The generation key made for issuing the certificate shall be used only for the issuance of the certificate.
◯ The generation key made for verifying the time of the document existence shall be used only for the intended purpose.

○ The generation key made for verifying the Online Certificate Status Protocol (OCSP) of the certificate shall be used only for the verification of the certificate.

1.3.3.1.5 Notice and Action on Important Facts

In the event of having a fact that effects gravely on the reliability and validity of certificate including damage, exposure, loss, stolen and others on generation key, pursuant to Article 21 (Management of digital signature generating information) of the Digital Signature Act, or having a fact that effects greatly on the certificate work of SignKorea under Article 9 (Transfer of Certification Work), Article 10 (Cancellation and Repeal of Certification Work), Article 12 (Suspension of Designation Cancellation of Certification Work), and Article 27-2(Mutual Recognition) of the Digital Signature Act, SignKorea shall promptly report the applicable fact to the Ministry of Public Administration and Security and the Korea Information Security Agency and shall take legal actions pursuant to Article 6 (Report of Acquisition and Merger) and Article 7 (Report of Suspension and Revocation of Certification Work) of the Implementation Regulation of the Digital Signature Act. In addition, the applicable facts shall be notified by using the homepage of SignKorea in principle, and if needed, may be notified via e-mail.

SignKorea shall seek ways to minimize the damage to subscribers and users after the notice to promptly take action.

1.3.3.1.6 Compliance of Pertinent Laws and Regulation and Rules

When performing the certification service, SignKorea shall comply with the relevant regulations of the Digital Signature Related Act and rules of the Korea Information Security Agency.

1.3.3.1.7 Guarantee on Verification Information

SignKorea confirms the fact only for the minimum of information needed to provide certification service from the information submitted by the subscriber, and guarantee the genuine fact on the applicable information to user. However, SignKorea does not take responsibility on the unverified information that SignKorea did not confirm, and the subscriber shall take full liability on the loss or damage incurred to the subscriber, user and SignKorea because a subscriber did not inform to SignKorea in spite of the change of information.

1.3.4 Subscriber

Pursuant to certain procedures determined under the regulation of SignKorea, it means that the subscriber joins the certification service of SignKorea and generates the digital signature generation key (hereinafter referred to as “generation key”) and digital signature verification key (hereinafter referred to as “verification key”) appropriate to the specification determined by SignKorea, and it further means the natural person (hereinafter referred to as "individual") and

corporation, organization and individual business enterprise (hereinafter collectively referred to as "corporate entity") who wishes to confirm the consistency of the generation key and verification key through the certificate issued by SignKorea on the information related to the verification key. However, in the event of a decision through the need of SignKorea, the information and communication equipment that performs the works on behalf of the subscriber may be included.

1.3.4.1 Responsibility and Obligation of Subscriber

1.3.4.1.1 Selection of Appropriate Certification and Providing Accurate Information

Subscriber shall select and apply for certificate appropriate to its own objective and understand correctly the Rules in relation to the application of the certification service, and shall provide accurate information and facts to SignKorea.

Subscriber shall fully be liable to users for the loss arising by the mistaken information of subscriber for the verification of digital signature by using the applicable certificate or relying on the information contained in the certificate.

1.3.4.1.2 Protection of Generation Key

Pursuant to Article 21 (Management of Digital Signature Generation Key), the subscriber shall protect the generation key as follows.

◯ A subscriber shall not allow the generation key to be misappropriated by using the password of an digital signature that only he/she knows.
◯ A subscriber shall be liable for the security of physical storing media such as hard disc or diskette, and smart cards where the generation key is stored.

The full responsibility of result from non-performance of obligation to protect on the above generation key shall be on the subscriber.

1.3.4.1.3 Appropriate Action

A subscriber shall notify the applicable facts to SignKorea or Registration Agency promptly if the following situation occurs and take appropriate action.

○ In the event of having a change on the information that SignKorea confirmed including the personal information (name, address, e-mail address and others) of the subscriber
○ In the event that the certificate is not to be used due to the arrest, death and others of the subscriber

○ In the event the generation key of the subscriber is released or damaged due to the release of password or stolen smart card or diskette
○ In the event that a third party other than the certificate subscriber attempts the issuance, suspension, reinstatement, renewal, re-issuance, or revoke

If the above situation occurs, the subscriber shall take the following action.

○ A subscriber shall be issued new certificate in the event of suspending the service for certificate of subscriber by requesting to SignKorea or Registration Agency for the revoke or re-issuance of the applicable certificate.
○ However, in the event that there is no way of proving the identity of the subscriber including arrest or death, the agent may bring the verifying document on the factual relationship and work on behalf of the subscriber.

SignKorea shall not be liable for the problems arising to the subscriber since the subscriber does not perform the above action.

1.3.4.1.4 Compensation Responsibility

Subscriber shall compensate the loss to SignKorea and user in the event that it incurred a loss to SignKorea and user intentionally or maliciously by using fraudulent practice or use of false digital signature and others.

1.3.4.1.5 Caution

In the event that subscriber applies to abolish via on-line, SignKorea uses the certificate management program for subscriber (hereinafter referred to as “management program”) and destroys the subscriber generation key and certificate of the storing device in principle. But, the generation key and certificate that the subscriber separately backed up shall be destroyed by the subscriber and all the liabilities arising from not performing it shall be on the subscriber.

1.3.5 Agent

Agent refers to the individual (executor, legal guardian, etc.) or corporation that the subscriber has designated or consented to. An agent may apply the certification service on behalf of a subscriber only in the case of having the verifying document such as the power of attorney or will of the subscriber, but cannot make the digital signature on behalf of a subscriber.

Under this Regulation, an Agent is included in the subscriber, and only in the case of needing a distinction on the subscriber and agent on contents, the subscriber and agent are separately specified.

1.3.6 User

User refers to the individual and corporate entity that wishes to confirm the generation key and verification key of subscriber by using the certificate issued by SignKorea.

1.3.6.1 Responsibility and Obligation of User

1.3.6.1.1 Understanding of Use Purpose of Certification

A user shall accurately understand the use purpose and scope of use on the certificate of subscriber. A user shall make the decision if the certificate of SignKorea that subscriber sent is appropriate to the objective of the user and the damages incurred by the mistake of the user is the liability of the user.

Confirmation of Contents and Effectiveness of Certification

Before using certificate, a user shall confirm the contents listed on the certificate of subscriber and the certificate of the KISA and SignKorea on the effective period and use, and shall confirm whether each certificate is suspended for validity or revoke through the certificate revocation list (hereafter referred to as the "CRL") or Real-time Certificate Status Information (Online Certificate Status Protocol, OCSP).

1.3.6.1.3 Recognition on Applicable Responsibility Clause and Guarantee

A user shall accurately recognize the contents including the validity of certificate and scope of guarantee, pertinent responsibility provision and others.

1.3.6.1.4 Compensation Responsibility of User

A user shall compensate for loss to SignKorea and the subscriber in the event it incurs loss to SignKorea and the subscriber in intentional or malicious method including fraud or falsified digital signature.

1.3.7 Relay Service Agency

Relay Service Agency refers to a party that concludes an agreement with SignKorea and Registration Agency to administer a system that simply delivers information registered by subscribers (hereinafter referred to as “relay system”).

1.3.7.1 Responsibility and Obligation of Relay Service Agency

1.3.7.1.1 Understanding of the Certification Practice Statement

Relay Service Agency shall fully understand the Rules, shall be responsible for complying with the matters specified by the agreement with SignKorea for the relay service, and for delivering the following information as it was transmitted by SignKorea as well as Registration Agency. Furthermore, Relay Service Agency has no authority to decode or retain any of the following information. Relay Service Agency shall be held accountable for damages to SignKorea, Registration Agency, subscriber(s) and user(s) caused by errors and defects in the relay service.

○ Information registered by a subscriber including the name of subscriber (full name or corporate name), Identification number (Korean resident registration number or business registration number), Address, Contact number, E-mail address, DN(Distinguished Name) and others
○ Reference number or license code created by SignKorea

1.3.7.1.2 Responsibility and Obligation of Relay Service Agency

In the event that Relay Service Agency delivers the information registered by subscribers to SignKorea, it should have the relay system and protection facilities pursuant to the Regulation on Protection Measures for Certification Authority for the following matters.

○ Restricted access
○ Monitoring of physical infiltration
○ Protection of the system and the network

Moreover, Relay Service Agency should report its plan for establishment and revisions to its relay system to the Minister of Public Administration and Security to obtain the approval on its adequacy. Similarly, Agency should record and retain the records on changes and revisions to the relay system and protection facilities. In addition, Relay Service Agency should go through a regular maintenance on safety by the Korea Information Security Agency at least once a year for its relay service-related systems and the overall management status.

1.3.7.1.3 Compensation Responsibility

In the event that Relay Service Agency causes adverse effect on the credibility of SignKorea via an intentional or malicious method or incurs monetary damage, Agency must indemnify SignKorea for such damages. In the event that Relay Service Agency causes damage to subscribers or users due to errors in its system, Agency shall be held accountable for it and make compensations.

1.3.7.1.4 Compliance of Certification Practice Statement

Relay Service Agency shall have responsibility for undertaking its work specified in this Practice Statement in a dutiful manner in regard to the offering of the certification service.

1.3.7.1.5 Protection of Subscriber’s Personal Information

Relay Service Agency shall be obligated to protect the personal information and other relevant

data of subscribers which are object of its relay service and to maintain its secured status.

1.3.8 Registration Agency

1.3.8.1 Responsibility and Obligation of Registration Agency

1.3.8.1.1 Accurate Identification

Registration Agency shall fully understand the rules, and has responsibility for the accuracy of identification of the subscriber. Registration Agency shall have responsibility for losses to the subscriber, user and SignKorea caused by the error and mistake of the identification result.

1.3.8.1.2 Notice on Important Facts

When the application for certificate is received, Registration Agency shall make the subscriber understand fully the important matters related to the use of the certificate, and if necessary, it shall obtain the confirmation of affixing the seal or signature of the subscriber.

1.3.8.1.3 Compensation Responsibility of Registration Agency

In the event of effecting negatively on the credibility of SignKorea or incurring monetary losses negligently or intentionally, Registration Agency shall compensate the losses, and it shall also compensate for the loss incurred on subscriber or user arising due to the identification error of certificate subscriber and others.

1.4 Management of the Certification Practice Statement

1.4.1 Name and Contact Information of the Supervising Department (or Supervising Manager) of the Practice Statement

Accredited Certification Center of SignKorea (English name: SignKorea)

○ Internet URL: http://www.signkorea.com
○ E-mail: signkorea@signkorea.com
○ Telephone: 1577-7337
○ Fax: 02) 767-7390

1.4.2 Cause and Procedure of the Establishment and Revision of Rules

SignKorea shall revise the Rules in the following cases.

○ In the event the Minister of Public Administration and Security orders to change the Rules pursuant to Clause 2 of Article 6 (Rules on Certification Works) of the Digital Signature Act
○ In the event SignKorea considers that the supplement or revision is necessary to reflect new works or to improve certification service

In the event that the Rules are revised, SignKorea shall maintain and manage a record on the details of the revision including the version, cause, details and others.

SignKorea shall obtain the internal confirmation and report it to the Ministry of Public Administration and Security based on Article 6 (Rules of Certification Works) of the Digital Signature Act. SignKorea shall complete the procedure of the report on revision before notifying its subscribers.

1.4.3 Notice and Implementation of Rules and Method of Subscriber Agreement

SignKorea shall notify the Rules in accordance with the following procedure.

◯ The revised Rules are granted with a new version.

◯ The revised Rules shall be immediately notified on the location of information storage specified below.

◯ Location of information storage for SignKorea Rules: http://www.signkorea.com/cps.html

SignKorea shall deem the amendment of rules as agreed in the event that subscriber does not request to revoke his or her accredited certificate within 2 weeks after the subscriber is notified of the Rules.

1.5 Terminology and Abbreviations

○ DN(Distinguished Name)

Distinguished Name, or DN for short, refers to the naming form which complies with the technical standards of the Regulation on the Facilities and Equipment of the Accredited Certification Authority, which is used for identifying the issuer and the owner of the certificate.

○ Subscriber

Subscriber refers to those who have issued the accredited certificate of their own for the digital signature verification key by the Accredited Certification Authority.

○ Accredited Certification Authority

Accredited Certification Authority refers to the entity that provides the accredited certificate service designated by the Minister of Public Administration and Security pursuant to Article 4 of the Digital Signature Act.

○ Service Interference Attack

Service Interference Attack refers to an act of attack which aims to interrupt the normal function of the system.

○ Trusted Party

Trusted Party refers to an act by the Korea Information Security Agency to identify the authenticity of the accredited certificate institution, the applicant and the submitted information in the process of issuing, renewing, suspending or abolishing the accredited certificate so as to secure its reliability.

○ Real Name

Real Name refers to the name displayed on the Korean resident registration table, on the business registration certificate and those which can be deemed as genuine pursuant to the Act on Act on Real Name Financial Transactions and Guarantee of Secrecy and the enforcement ordinance under the same act.

○ Certification

Certification refers to an act of identifying and proving that the verification key for digital signature is consistent with the generation key for the digital signature that a natural person or a corporation possesses.

○ Digital Signature Certification Scheme

Digital Signature Certification Scheme refers to a scheme which provides certification works which include issuance of certificate and management of records in relation to certificate.

○ Accredited Certificate

Accredited Certificate refers to the digital information which identifies and proves the fact that the verification key for digital signature is consistent with the generation key for the digital signature that a natural person or a corporation possesses.

○ Accredited Certification Work

Accredited Certification Work refers to general service which provide relevant works which include issuance of certificate and management of records in relation to certificate.

○ Digital Document

Digital Document refers to information which is prepared, transmitted, received or stored in the digital form by the device that has the information processing capability such as a computer.

○ Digital Signature

Digital Signature refers to the information generated by the generation key of digital signature through the asymmetric encryption so as to identify the party that has drawn up the digital document and to examine whether the digital document has been revised. It is the unique indication of the digital document concerned.

○ Generation Key of Digital Signature

Generation Key of Digital Signature refers to information in the digital form which is used to generate digital signature.

○ Verification Key of Digital Signature

Verification Key of Digital Signature refers to information in the digital form which is used to verify digital signature generated by the Generation Key of Digital Signature.

○ Digital Signature Key

Digital Signature Key refers to the Verification Key of Digital Signature which is consistent to the Generation Key of Digital Signature.

○ Certification Authority

Certification Authority refers to a system that provides a functional or technical support to management of registered information, creation/management of digital signature key, creation/issuance of accredited certificate and the time stamp service (verification on the point where the document started to exist).

2. Types and Service Fees of Accredited Certificate

2.1 Types of Accredited Certificate

The period of effectiveness of accredited certificate issued by SignKorea is limited to 1 year, and shall prescribe specific period starting from the day of subscriber's application or issuance. However, the effective period of reissued or renewed certificate can be extended or shortened from the designated expiry period of 1 year in accordance with [Table 1].

Classification	Effective period
New issuance	1 year
Reissuance	Remaining period
Renewal	Remaining period + 1 year

[Table 1] Certificate Effective Period

SignKorea makes the classification as in [Table 2] for the grade of certificate depending on the scope of use for certificate and use. However, SignKorea considers the risk following the frequency of use and may classify in detail for certain grades.

Grade	Scope of Use and Usage
Special	.Identification and electronic signature in the non-face-to face situation .Exchange of e-document at non-financial institution and financial institution

	.In the event the size of e-document for exchange is large or very important .Protection of communication channels
Platinum	.Identification and electronic signature in the non-face-to face situation .Exchange of e-document at non-financial institution and financial institution .Protection of communication channels ※ However, it may be classified depending on the risk and utilization
Gold	.e-business on the securities and insurance area .Government permitted area such as e-Services at the G4C
Silver	.Identification and electronic signature through the groupware between employees in a corporation .Use only for limited purposes for specific service or service provider .Government permitted area such as e-Services at the G4C

[Table 2] Grade of Certificate and Scope of Use

SignKorea recommends to use appropriately for the use and scope of use for each certificate grade as above, and shall not be held accountable whatsoever for any damages occurred by the inappropriate use for certificate grade by subscriber and user.

SignKorea shall issue the platinum grade in certificate for mutual interface, and OID of certificate shall be as follows for each issued person.

- Corporation, organization, sole proprietorship : 1.2.410.200004.5.1.1.7

- Individual : 1.2.410.200004.5.1.1.5

2.2 Service Fees of Accredited Certification

SignKorea may impose service fees on issuance of certificate to the subscriber and the user, use of certificate, and providing of other certification service. The service fees of SignKorea shall have new issuance and renewal of the existing certificate as subjects. Subscriber shall pay the fees which are determined in accordance with the subscriber and service fee grades before issuing the certificate in principle.

SignKorea determines the standard of fees for issuance as in [Table 3] depending on the grade, subject for issuance, and use of the certificate.

Fees (Unit: 1,000 won/year, VAT seperate)

Type / Grade	Individual Certificate		Corporate Certificate	
	For Work	For Server	For Work	For Server
Special	Under the separate agreement			
Platinum	4	500	100	1,000
Gold	Under the separate agreement			
Silver				

[Table 3] Issuance fees (based on one year of effective period)

SignKorea may apply the discount rate or exempt the fees pursuant to the policy of the government and SignKorea, and the fee imposing method or payment period may be changed by the agreement or stipulation with subscriber and user.

SignKorea may impose service fees on the certificate use and others in addition to the fees to issue the certificate when needed, and shall follow the separate agreement for fees following the use of time stamp service, verification service and others.

2.3 Refund

In the event that a subscriber visits SignKorea or Registration Agency, fills in the refund form and requests a refund within 7 days from the issuance of the accredited certificate, not using it, SignKorea may refund the fees. At this time, in the event the expenses are paid for reception and registration of the applicable certificate application, the applicable expenses are deducted from the fees and a refund is made.

3. Certifications Works including Issuance of Certification

3.1 Submission of Issuance Application

3.1.1 Application

The person who wishes to receive the certificate of SignKorea or its agent (hereinafter referred to as “Applicant”) shall possess the identification voucher following 3.15 (Data Submission for Identification by Certifications) and visit Registration Agency to submit the certificate application to Registration Agency.

3.1.2 Application for Issuance

Registration Agency distributes to the Applicant the certificate registration confirmation listed with the reference number and permission code after the identification procedure (including online identification) under 3.2.1 (Identification in the Process of New Issuance).

When the Applicant enters the reference number and permission code on the management program provided through the homepage of SignKorea or Registration Agency, the management program generates the digital signature key and applies the issuance of certificate to SignKorea.

3.1.3 Period for Certification Processing

The reference number and permission code issued to the subscriber by SignKorea via its system or Registration Agency shall be effective for the designated period specified in the [Table 4] depending on the type of the accredited certificate.

Type / Period for Issuance	Individual Certificate		Corporate Certificate	
	For Work	For Server	For Work	For Server
After registering certificate	25 days	25 days	25 days	25 days

[Table 4] Period for Issuing Certificate

Note that the issuance of the accredited certificate can be postponed or rejected in the event that there is an issue with the accuracy and reliability of the information submitted by subscriber or subscriber refuses to pay the service fee for issuance. In the event that the number of subscribers is large, including group subscription, processing time may take longer than usual.

3.2 New Issuance of Accredited Certificate
3.2.1 Identification in the Process of New Issuance

When a subscriber lists the matters determined on 3.15 (Data Submission for Identification by Certifications) on the application and submits the necessary verification data, Registration Agency shall compare the identification voucher and the subscriber to confirm the identity and process the application. At this time, in the event that an agent files for application, the power of attorney and the identification voucher of the recipient shall be confirmed.

In the event that a subscriber who has already received certificate from the certification authority is to issue a new certificate, the identity of the applicable subscriber may be verified by the digital signature and certificate of the applicable subscriber. In this event, the certificate of the applicable subscriber shall be effective at the time the identity of subscriber is verified by the certification authority and others.

3.2.2 Name Used in Certificate

In order to distinguish the subscriber, SignKorea uses subscriber distinction information (hereinafter referred to as "DN") that is in an appropriate form for the specification or the technology standard related to DN (Distinguished Name) determined by ITU-T X.500.

SignKorea permits its legal name as follows in issuing the certificate. However, only when a subscriber desires the nickname and others, SignKorea may permit the desired name on the certificate.

- Real name, corporation name and other legal name
- Trade-mark right obtained from Patent and Intellectual Property Office, or equivalent institutions of other countries (requires verification statement)
- Internet domain name
- Internet IP address
- URL for WWW
- E-mail address, etc.

SignKorea structures the name and other information that the subscriber submitted in DN to store in the certificate. DN becomes standard information when the user confirms the certificate that the certificate is issued only when the duplication of the DN of new subscriber and the DN of the existing subscriber is not overlapped.

In the event the DN is overlapped, SignKorea shall request a new DN to the subscriber, and the subscriber shall respond to it to subscribe to the certification service of SignKorea. SignKorea does not apply special interpretation regulation for accommodating various names.

SignKorea shall not be liable for resolving problems if the existing subscriber uses the legal name of a new subscriber on the DN to cause litigation or dispute.

3.2.3 Generation and Issuance of Certificate

In the event that SignKorea receives the information of a subscriber who wishes to issue the accredited certificate through Registration Agency or Relay Service Agency via information communication network, the confidentiality and integrity of the subscriber's information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

After receiving the application for issuing the accredited certificate, SignKorea shall identify that the generation key of digital signature is exclusive to the subscriber concerned by verifying the information submitted for issuance application which has been signed by the generation key of digital signature by the subscriber.

SignKorea shall generate and issue the certificate following X.509 Version 3 by digital signature with the generation key of SignKorea for the DN and verification key of the applicant and records the certificate on the directory.

3.2.4 Acquisition of Certification

The Applicant receives the certificate generated by SignKorea through the management program and selects the media to store the generation key and the certificate, and safely stores it. Acquiring of certificate by the subscriber means the guarantee that the following facts are true to the users and SignKorea from the time of generating the certificate to the effective period.

○ No illegal user gains the access to the generation key of subscriber.
○ Matters confirmed by SignKorea on all information in certificate are true.
○ Matters that subscriber notified to SignKorea in addition to the information in the certificate are true.
○ Certification is used only within the scope determined by SignKorea under the rules.

Applicant who acquired the certificate of SignKorea becomes the subscriber of SignKorea. Acquiring the certificate of SignKorea by the Applicant means that it will not incur damages to SignKorea and users with the following and agrees that it will compensate for the damages.

○ Providing false fact of subscriber or its agent
○ Lack of notice of important facts due to the negligence or malicious intent of subscriber
○ Loss, damage, stolen or disclosure of generation key of subscriber

SignKorea considers that it agrees to the above contents for subscriber and agent in the event the certificate is acquired by the agent of the subscriber.

3.3 Renewal of Certificate

Renewal of certificate refers to the issuance of a new certificate in the same type with its digital signature information and expiry date renewed followed by its expiration.

SignKorea does not change subscriber information other than the effective period during the course of the renewal process. At this time, the generation key for subscriber is changed and the existing certificate is abolished.

3.3.1 Identification in the Renewal Process

SignKorea newly issues the certificate for a new effective period when the subscriber submits renewal application via online to SignKorea that includes the digital signature. The effective period of newly issued certificate includes the remaining effective period of the existing effective period. At this time, the identification on subscriber is replaced with the verification of digital signature.

In the event that SignKorea receives the information of a subscriber who wishes to issue the accredited certificate through Registration Agency or Relay Service Agency via information communication network, the confidentiality and integrity of the subscriber's information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

After receiving the application for renewing the accredited certificate, SignKorea shall identify that the generation key of digital signature is exclusive to the subscriber concerned by verifying the information submitted for renewal application which has been signed by the generation key of digital signature by the subscriber.

3.3.2 Issuance and Registration of Certification

SignKorea shall immediately record the applicable certificate to the directory immediately after issuing the renewed certificate of the subscriber, and the existing certificate is deleted from the directory.

3.3.3 Period of Renewal Application

In the event that remaining effective period before expiration is less than one month, SignKorea principally renews the subscriber certificate. However, SignKorea may adjust the application period considering the convenience of subscriber.

3.4 Re-issuance of Certification

In the event that the subscriber applies for a new certificate due to security problems after his/her generation key of digital signature has been lost, damaged, stolen or disclosed, SignKorea may abolish his/her existing accredited certificate and issue a new one.

SignKorea shall set the expiry period of the new accredited certificate as the remaining period of the existing certificate, and finalizes the process of issuing a new certificate through a new generation key and the digital signature on the existing DN.

3.4.1 Application for Re-issuance

Application for re-issuance can be personally made by the subscriber requesting for re-issuance through the digital signature via on-line, and the re-issuance is made after requesting the re-license of SignKorea since the re-issuance by on-line digital signature is impossible.

In the event of re-issuance using the digital signature, the subscriber possessing the certificate of SignKorea shall apply for re-issuance to SignKorea through the management program via on-line. In the event of re-issuance by using the re-license, they shall follow the procedure of applying for a new issuance of the certificate.

In the event that SignKorea receives the information of a subscriber who wishes to re-issue the accredited certificate through Registration Agency or Relay Service Agency via information communication network, the confidentiality and integrity of the subscriber's information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

After receiving the application for re-issuing the accredited certificate, SignKorea shall identify that the generation key of digital signature is exclusive to the subscriber concerned by verifying the information submitted for re-issuance application which has been signed by the generation key of digital signature by the subscriber.

3.4.2 Identification in the Re-issuance Process

SignKorea replaces the digital signature verification with the identification of a subscriber for the re-issuance process based on the digital signature. SignKorea shall follow the procedure for new issuance in the event of re-issuance through re-license.

3.5 Modification in Subscriber's Registered Information

In the event that a subscriber's information reflected in the certificate shall be modified, it shall follow the procedure of 3.2 (New Issuance of Accredited Certification). In the event of modifications in the subscriber information other than the above (e.g., address, contact number, e-mail address, and so on), a subscriber may request modification in the registered information for SignKorea to update the information concerned.

3.5.1 Modification Request for Subscriber Information

A subscriber shall submit application for information modification via online. SignKorea shall identify the subscriber via his/her digital signature included in the application.

In the event that SignKorea receives the information of a subscriber who wishes to modify the registered information via information communication network, the confidentiality and integrity of the subscriber's information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

After receiving the application for issuing the accredited certificate, SignKorea shall identify that the generation key of digital signature is exclusive to the subscriber concerned by verifying the information submitted for issuance application which has been signed by the generation key of digital signature by the subscriber.

3.5.2 Acquisition of Certificate

A subscriber shall follow the method specified in 3.2.4 (Acquisition of Certification) to receive the accredited certificate with the updated information.

3.6 Suspension/ Restoration/ Repeal of Validity for Certificate

3.6.1 Suspension of Validity for Certificate

SignKorea promptly suspends the validity of certificate when requesting the suspension of validity in the following cases pursuant to Article 17 (Suspension of Validity of Certification) of the Digital Signature Act.

○ In the event of having a suspicion of loss, damage, stolen or disclosure of generation key of subscriber
○ In the event a subscriber desires to suspend the certificate of validity

SignKorea may suspend the certificate for certain time in the event an inevitable cause occurs for the management of certification service or is ordered for suspension by the right of the Minister of Public Administration and Security pursuant to Article 16 (Termination of Validity of Accredited Certification) of the Digital Signature Act.

SignKorea may suspend the validity of certificate for up to 6 months after the suspension pursuant to Article 17 (Suspension of Validity of Certification) of the Digital Signature Act, and in the event of sustaining for 6 months or longer, the certificate is revoked. However, in the event the effective period expires during the term of suspension, it shall be deemed the same as the expiration of the effective period of ordinary certificate.

3.6.1.1 Submission of Application for Suspending Effectiveness

The subscriber who possesses the certificate of SignKorea may suspend the effectiveness via on-line through the management program without visiting the Registration Agency, and may apply for the suspension through the Registration Agency in the event of applying via on-line due to the cause of subscriber.

In the event that SignKorea receives the information of a subscriber who wishes to suspend the effectiveness of the accredited certificate through Registration Agency or Relay Service Agency via information communication network, the confidentiality and integrity of the subscriber’s information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

3.6.1.2 Identification

Registration Agency shall indentify subscribers pursuant to 3.2.1 (Identification in the Process of New Issuance). In the event of the subscriber applying for the suspension of validity via on-line to SignKorea, SignKorea replaces the identification with the digital signature of the subscriber.

3.6.1.3 Effect

In the event the subscriber suspends the validity of certificate, SignKorea shall promptly suspend the validity regardless of the effective period and types of certificate, but there is no validity on the effects and obligations of contract or legal conduct that the subscriber has performed before the suspension.

3.6.2 Restoration of Validity for Certificate

SignKorea shall restore the validity of certificate in the event subscriber applies for validity reinstatement of certificate to SignKorea for modifying the validity of certificate within 6 months after suspending the validity and restoring the validity of certificate by SignKorea, due to the inevitable cause of certification service operation under the decree of the Ministry of Public Administration and Security under the provision of Article 16 (Termination of Validity of Accredited Certification) of the Digital Signature Act.

SignKorea considers the digital signature made with the generation key that is consistent with the verification key of the suspended certificate as not having legal validity, and the subscriber can not apply for the reinstatement of validity to SignKorea via on-line. Therefore, the subscriber shall visit Registration Agency and apply for reinstatement of the validity.

3.6.2.1 Procedure

The subscriber who possesses the certificate of SignKorea may suspend the effectiveness via on-line through the management program without visiting the Registration Agency, and may apply for the suspension through the Registration Agency in the event that online application is impossible due to the cause of the subscriber.

In the event that SignKorea receives the information of a subscriber who wishes to restore the validity of the accredited certificate through Registration Agency or Relay Service Agency via information communication network, the confidentiality and integrity of the subscriber’s information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

3.6.2.2 Identification

Registration Agency shall indentify subscribers pursuant to 3.2.1 (Identification in the Process

of New Issuance).

3.6.3 Revocation of Certificate

SignKorea may revoke the certificate of the subscriber with the following causes pursuant to Article 18 (Repeal of Certification) of the Digital Signature Act.

○ In the event the subscriber wishes to abolish the certificate
○ In the event that the fact of loss, damage, theft or disclosure on the generation key of the subscriber is detected
○ In the event that the fact of death, report on missing or dissolution of the subscriber is detected
○ In the event that the fact of illegal issuance of the certificate for the subscriber is detected
○ In the event that the subscriber violates important obligations under the rules
○ In the event the compliance of the obligations of the subscriber is delayed or becomes impossible due to natural disaster or other causes
○ Certification issuance due to error or other inadvertent acts

3.6.3.1 Submission of Revocation Application

The subscriber who possesses the certificate of SignKorea may apply for revoke via online through the management program without visiting Registration Agency, and in the event that online application is impossible due to the cause of the subscriber, the revoke application may be made through Registration Agency.

In the event that SignKorea receives the information of a subscriber who wishes to suspend the effectiveness of the accredited certificate through Registration Agency or Relay Service Agency via information communication network, the confidentiality and integrity of the subscriber's information shall be guaranteed by the digital signature certification of the Registered Agency and the encryption pursuant to the cryptographic algorithm in the No. 3, Paragraph 1 under Article 5 of the Regulation on the Facilities and Equipment of the Accredited Certification Authority .

3.6.3.2 Identification

Registration Agency shall indentify subscribers pursuant to 3.2.1 (Identification in the Process of New Issuance). In the event of the subscriber applying for the revoke via on-line to SignKorea, SignKorea replaces the identification with the digital signature of the subscriber.

3.6.3.3 Effect

SignKorea shall promptly revoke the validity regardless of the effective period and type of certificate in the event the subscriber revokes the validity of certificate. However, validity is not given to the obligations and validity on the legal actions or contract performed by the subscriber before the revoke.

3.6.4 Issuance Interval and Expected Time of Notice for Certification Revocation List (CRL)

The Certification Revocation List (CRL) shall be issued on maximum 24-hour interval, and the status information shall be modified as immediately as possibly from the point of issuance.

3.7 Real-time Certificate Status Information (Online Certificate Status Protocol, OCSP).

3.7.1 Directions

An applicant or his/her agent for the Real-time Certificate Status Information (hereinafter referred to as “OCSP”) should apply for service subscription to SignKorea in advance. A service subscriber or user to OCSP shall request for the OCSP via the OCSP client software provided by SignKorea or his/her software which is available for requesting/processing OCSP.

3.7.2 Requirements

Both OCSP and its client software provided by SignKorea is paid service and the specific rates shall be determined in accordance with a separate consent. In addition, a subscriber or user who makes a request for OCSP via online is required to make an digital signature via his/her generation key of digital signature and accredited certificate, and to comply with the RFC2560 when making a request for OCSP for the purpose of a standardized process.

3.7.3 Termination of Service Agreement

A subscriber or user to the OCSP service has the right to terminate the service agreement via a designated process with SignKorea.

3.8 Miscellaneous Additional Service

In the event that a subscriber or a user requests the time stamp service for digital document (verification on the point where the document started to exist), SignKorea shall offer the requested service. Note that the applicant above should bear service fees and other necessary costs. Specific terms of use and termination of service agreement shall be determined separately by the consent of SignKorea.

As for the time stamp service, SignKorea operates a receiver for satellite time for the purpose of providing the international standard time information accurately.

3.9 Accredited Certificate Profile

The accredited certificate issued by SignKorea shall include the followings pursuant to Article 15-2 of Digital Signature Act, and shall comply with the technical standards of the digital signature certificate profile which are those of the digital signature certification scheme of Korea as with [Table 5].

○ Name of a subscriber (Refers to the company name in the event of corporate)

○ Information on the digital signature verification of a subscriber
○ Digital signature method used by a subscriber and an accredited certificate institution
○ Serial number of the accredited certificate
○ Expiry period of the accredited certificate

○ Information for verifying the entity is the valid accredited certificate institution such as the name of the accredited certificate institution
○ Matters regarding the scope of use or restricted usage of the accredited certificate if any
○ Matters regarding the fact that a subscriber holds the right of representation for the third party or has requested indication of the vocational entitlement if nay
○ Indication that shows the status as an accredited certificate

■ Basic Fields

	Name of Field	Type of ASN.1	Note	Support		Remarks
				Creation	Processing	
1	Version	INTEGER	0x02 (Version 3)	m	m	
2	Serial Number	INTEGER	Automatic allocation	m	m	
3	Issuer	OID	[KCAC.TS.DN] compliance C(Country) is printableString, the property figures for others are utf8String	m	m	
	type	OID		m	m	
	value	printableString		m	m	
		or utf8String				
4	Validity		Duration of certificate	m	m	
	notBefore	UTCTime		m	m	
	notAfter	UTCTime		m	m	
5	Subject		[KCAC.TS.DN] compliance C(Country) is printableString, the property figures for others are utf8String	m	m	
	type	OID		m	m	
	value	printableString		m	m	
		or utf8String				
6	Subject Public Key Info			m	m	
	algorithm	OID	Compliance with technical standards of digital signature certification system algorism	m	m	
	subjectPublicKey	BIT STRING		m	m	

7	Extentions	Extentions		m	m	

■ Extension Fields

	Name of Field	Type of ASN.1	Note	C	Support		Remarks
					Creation	Processing	
1	Authority Key Identifier			n	m	m	
	keyIdentifier	OCTET STRING	KeyID of issuer certificates		m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	160 bit hash figures of subjectPublicKey data	n	m	m	
3	Key Usage	BIT STRING	Digital signature, Non-repudiation	c	m	m	
4	Certificate Policy			c	m	m	
	policyIdentifier	OID	Certificate policy		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	
	Qualifier				m	m	
	Qualifier				m	m	
	CPSuri	IA5String	URI of CPS		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	Compliance with indication standards of accredited certificates		m	m	
5	Policy Mappings			-	-	-	
6	Subject Alternative Names	otherName	Korean real name and VID of subscriber in id-kisa-identifyData	n	m	m	
		rfc822Name			o	m	
7	Issuer Alternative Names	otherName	Korean real name of accredited certification authorities in id-kisa-identifyData	n	o	m	
8	Extended Key Usage	OID	id-kisa-HSM	n	o	o	
9	Basic Constraints			-	x	x	
10	Policy Constraints			-	-	-	
11	Name Constraints			-	-	-	
12	CRL DistributionPoint			n	m	m	
	distributionPoint	DistributionPointName	CRL acquisition data		m	m	
	reasons	ReasonFlags			-	-	
	cRLIssuer	GeneralNames	Used in indirect CRL issuance		o	m	
13	Authority Information Access			n	m	m	
	accessMethod	OID	id-ad-ocsp		m	m	

	accessLocation	GeneralNames	OCSP URI		m	m	

[Table 5] User Digital Signature Certificate Profile

3.10 Certificate Revocation List (CRL) Profile

SignKorea generates the Certification Revocation List in the event of suspending, restoring or revoking the accredited certificate of a subscriber. SignKorea shall comply with the technical standards of the CRL profile of the digital signature certification which are those of the digital signature certification scheme of Korea as with [Table 6].

■ Basic Fields

	Name of Field	Type of ASN.1	Note	Support		Remarks
				Creation	Processing	
1	Version	INTEGER	0x01 (Version 3)	m	m	
2	Signature	OID		m	m	
3	Issuer		[KCAC.TS.DN] compliance C(Country) is printableString, the property figures for others are utf8String	m	m	
	type	OID		m	m	
	value	printableString or utf8String		m	m	
4	This Update	UTCTime	Creation time of CRL	m	m	
5	Next Update	UTCTime	Expected time of the following renewal of CRL	m	m	
6	Revoked Certificates			m	m	
	userCertificate	INTEGER		m	m	
	revocationData	UTCTime		m	m	
	crlEntryExtensions	Extensions		m	m	
7	CRL Extensions	Extensions		m	m	

■ CRL Extension Fields

#	Name of Field	Type of ASN.1	Note	C	Support		Remarks
					Creation	Processing	
1	Authority Key Identifier			n	m	m	
	keyIdentifier	OCTET STRING	KeyID of certificates of certification authorities		m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Issuer Alternative Names	otherName	Korean real name of accredited certification authorities in id-kisa-identifyData	n	o	m	
3	CRL Number	INTEGER		n	m	m	
4	Issuing DistributionPoint			c	m	m	
	DistributionPointName	IA5String	CRL acquisition data		m	m	
	onlyContainsUserCerts	BOOLEAN			-	-	

	onlyContainsCACerts	BOOLEAN			-	-	
	onlySomeReasons	BIT STRING			-	-	

■ CRL Entry Extension Fields

	Name of Field	Type of ASN.1	Note	C	Support		Remarks
					Creation	Processing	
1	Reason Code	ENUMERATED		n	m	m	
2	Hold Instruction Code	OID		n	o	m	
3	Invalidity Date	UTCTime		n	o	m	
4	Certificate Issuer	GeneralNames		C	o	m	

[Table 6] User Digital Signature Certificate CRL profile

3.11 Certificate Profile for the Real-time Certificate Status Information (OCSP) Service

The certificate for the OCSP server which is used to verify the effectiveness of a subscriber's accredited certificate complies with the technical standards of the certificate profile of the digital signature certification which are those of the digital signature certification scheme of Korea as with [Table 7].

■ Basic Fields: Same as the certificate profile for a subscriber's digital signature

■ Extension Fields

	Name of Field	Type of ASN.1	Note	C	Support		Remarks
					Creation	Processing	
1	Authority Key Identifier		Use all three figures/td>	n	m	m	
	keyIdentifier	OCTET STRING			m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	160 bit hash figures of subjectPublicKey data	n	m	m	
3	Key Usage	BIT STRING	Digital signature, Non-repudiation	c	m	m	
4	Certificate Policy			c	m	m	
	policyIdentifier	OID	Certificate policy		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	

	Qualifier				m	m	
	CPSuri	IA5String	URI of CPS of accredited certification authority that has issued OCSP certificate		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	Compliance with indication standards of accredited certificates		m	m	
5	Policy Mappings			-	-	-	
6	Subject Alternative Names	otherName	Korean real name and VID of subscriber in id-kisa-identifyData	n	m	m	
7	Issuer Alternative Names	otherName	Korean real name of accredited certification authorities in id-kisa-identifyData	n	o	m	
8	Extended Key Usage	OID		c	m	m	
9	Basic Constraints			-	x	x	
10	Policy Constraints			-	-	-	
11	Name Constraints			-	-	-	
12	CRL DistributionPoint			n	m	m	
	distributionPoint	DistributionPointName	CRL URI		m	m	
	reasons	ReasonFlags			o	m	
	cRLIssuer	GeneralNames	Used in indirect CRL issuance		o	m	
13	Authority Information Access			n	o	m	
	accessMethod	OID	d-ad-ocsp				
	accessLocation	GeneralNames					
14	OCSP No Check	OID	id-pkix-ocsp-nocheck	n	o	m	

[Table 7] The Accredited Certification Authority Time Stamp and OCSP Server Certificate Profile

3.12 Renewal of Digital Signature Key of the Accredited Certification Authority

3.12.1 Renewal Process

The accredited certificate by SignKorea can be renewed due to expired certificate of SignKorea and the need by the digital signature certification scheme. The renewal process shall comply with the 5.2 (Facilities of the Accredited Certification Authority for Generation and Management of Digital Signature Key) of the Regulation on the Facilities and Equipment of the Accredited Certification Authority.

3.12.2 Distribution Process of Renewed Certification

Certification of SignKorea shall be distributed in accordance with the following procedure for the purpose of safe use of a subscriber’s certificate.

○ Certification is renewed by SignKorea, the root certification authority.
○ Renewed certificate is accepted.
○ The renewed certificate is posted on the directory server of SignKorea.
○ Renewal status is notified to respective accredited certificate institutions and the renewed certificate is delivered.
○ Renewal status is notified to respective institutions that use the certificate and the renewed certificate is delivered.
○ After the renewed certificate is delivered, a subscriber's certificate is issued by the renewed generation key of the digital signature.

3.13 Discontinuance and Abolition of Accredited Certification Service

In the event that SignKorea should discontinue or abolish the entirety or part of its accredited certificate service due to unavoidable causes except for natural calamities or force majeure, SignKorea shall select the period of discontinuation and the specific dates for such discontinuance and revocation pursuant to Article 10 of the Digital Signature Act, and notify subscribers of the decision 30 days before the date of discontinuance and 60 days before the date of revocation via the online homepage of SignKorea or digital mails.

3.14 Cessation or Canceled Status of Accredited Certification Service

In the event that SignKorea's status as the accredited certificate institution is canceled pursuant to Article 12 (Cessation or Canceled Status of Accredited Certification Service) of the Digital Signature Act, SignKorea shall transfer the works to the other accredited certificate institution(s) promptly. Note that the work transfer is not possible due to the cause of the recipient accredited certificate institution, SignKorea shall submit relevant data including the statement of reason to the Minister of Public Administration and Security pursuant to Article 7 (Reports for Discontinuance of Accredited Certification Service) of the Enforcement Regulations of the Digital Signature Act.

3.15 Document Submissions by Accredited Certifications for Identification

SignKorea shall construct part of the information submitted by a subscriber in the DN form to include it in the accredited certificate, and prevent other information from being leaked outside as confidential information.

3.15.1 Individual Certification

3.15.1.1 Individual Identification Voucher

SignKorea uses one of the following as the identification voucher for individual identification.

○ Resident registration card for the person subject to resident registration cards. However, in the event it is difficult to rely on the resident registration card, the voucher can be confirmed by the attached photo with the listing of name and resident registration number that is issued by the head of the school under the National Institution, Local Government and Education Act
○ The certified copy of resident registration and identification voucher and document of legal agent for a person not subject for issuing the resident registration card

○ Foreigner resident registration under the Immigration Act for Foreigners. However, the identification voucher issued by the authorized administration of the applicable country or a passport in the event of a person not issued with a foreigner registration card

Individual Identification Chart shall abide by the Article 13-3 (Identification Certification Chart) of the Implementation Regulations of the Digital Signature Act.

3.15.1.2 Individual For Work Certification Identification

When applying for certification service for work by an individual subscriber, Registration Agency shall confirm the identity of subscriber by reviewing the application that is listed with one of the following items from 3.15.1.1 (Individual Identification Voucher).

○ Name
○ Korean resident registration number
○ DN
○ Usage and grade
○ Address
○ Telephone number
○ E-mail address
○ Institution and department
○ Securities account number or bank account number (only when necessary)
○ Other information that SignKorea requires

3.15.1.3 Individual For Server Certification Identification

When an individual subscriber applies for certification service for server, Registration Agency shall review the application listed in the following category and the individual identification voucher and confirm the identity of subscriber and existence of the server.

○ URL or IP
○ Name
○ Korean resident registration number
○ DN
○ Usage and grade
○ Address
○ Telephone number
○ E-mail address
○ Institution and department
○ Securities account number or bank account number (only when necessary)
○ Other information that SignKorea requires

3.15.2 Corporate Certificate

3.15.2.1 Corporate Identification Voucher

SignKorea uses one of the following as the identification voucher for corporate identification.

○ Certified copy of corporate registration or commercial registration under the Voluntary Matters Proceedings Act
○ Business registration under the Corporate Income Tax Act
○ Tax payment number under the Income Tax Act
○ Identification number and business registration certification under the Value Added Tax Act

Individual entrepreneurs shall confirm the identity with the 3.15.1.1 (Individual identification voucher) and individual business registration.

For a voluntary organization, the identity is confirmed with the identification voucher of the representative individual in the event of not having a tax number or ID number, and of the notice document of granting the tax number and ID number if there are a tax number and ID number.

The foreign corporation and voluntary organization located in a foreign country confirm their identity by applying for one of the following.

○ Copy of corporate registration or commercial registration issued by the pertinent authority of the applicable country
○ Identification related verification document including the document that may be recognized for the legal entity by the consul of the applicable country located in Korea or the authorization of the country certified.

3.15.2.2 Identification of Corporate Certificate for Work

When the corporate subscriber applies for the certification service for work, Registration Agency shall review the application listed with one of 3.15.2.1 (Corporate Identification Voucher) and the below information to confirm the identity of the corporation.

○ DN
○ Usage and grade
○ Quantity
○ Corporate name
○ Telephone number of enterprise
○ Address of business place of corporate entity
○ Securities account number or bank account number (only when necessary)
○ Position of the person in charge
○ Name and place of contact for person in charge
○ E-mail of person in charge
○ Other information needed by SignKorea

Note that the representative of the corporate concerned shall be identified pursuant to 3.15.1.1. In the event an agent applies, SignKorea shall add the following checklist to the normal procedure of identification for the agent concerned.

○ Agent's identification voucher pursuant to 3.15.1.1 (Individual Identification Voucher)
○ Power of attorney by the representative of the corporate
○ Affixing of corporate seal

3.15.2.3 Identification of Corporate Certification for Server

When the corporate subscriber applies for the certification service for server, Registration Agency shall review the application listed with one of 3.15.2.1 (Corporate Identification Voucher) and the below information to confirm the presence of the corporation and corporation server by confirming through a reliable third party institution. However, if the application is filed by an agent, the identity of the agent is confirmed after receiving the power of attorney of the representative from the agent.

○ URL or IP
○ DN
○ Usage and grade
○ Quantity
○ Corporate entity name
○ Telephone number of enterprise
○ Address of business place of corporate entity
○ Securities account number or bank account number (only when necessary)
○ Position of the person in charge
○ Name and place of contact for person in charge
○ E-mail of person in charge
○ Other information needed by SignKorea

In the event an agent applies, SignKorea shall add the following checklist to the normal procedure of identification for the agent concerned.

○ Agent's identification voucher pursuant to 3.15.1.1 (Individual Identification Voucher)
○ Power of attorney by the representative of the corporate
○ Affixing of corporate seal

4. Notices on Information Regarding Accredited Certification Service

4.1 Facility for Notice

SignKorea is the subject of operation on the facility for notice in relation to the information that regards the accredited certificate service such as the Certification Revocation List (hereinafter referred to as "Information Regarding Accredited Certification Service"). SignKorea shall post the Information Regarding Accredited Certification Service once a day or more frequently.

4.2 Methods of Notice

SignKorea shall post the Information Regarding Accredited Certification Service once a day or more frequently.
The locations for storing SignKorea's Information Regarding Accredited Certification Service are as follows:

○ Directory: ldap://dir.signkorea.com
○ Homepage: http://www.signkorea.com/data/totalcrl.tar.tar
○ Real-time Certificate Status Information: http://ocsp.signkorea.com

5. Control Procedure for Facility and Equipment of Accredited Certification Service

5.1 Control of Physical Approach

5.1.1 Matters on Compartments of Operations Office of the Certification System

SignKorea compartments the operations office of the certification system pursuant to the provisions of 8.2.1 (Operations Office of the Certification System) of the Regulation on the Facilities and Equipment of the Accredited Certification Authority promulgated by the Ministry of Public Administration and Security as follows:

○ While the facility for managing information registered by subscribers, that for managing generation keys of the digital signature by accredited certificate institution, and that for providing functions to generation/issuance of certificates can be installed in a same operations office altogether, they should be compartmented from other facilities for separate management.
○ The facility for providing functions of notice on accredited certificate should be compartmented from other facilities for separate management.
○ While the facility for providing functions of Real-time Certificate Status Information and that for providing functions of the time stamp service can be installed in a same operations office altogether, they should be compartmented from other facilities for separate management.

5.1.2 Control of Physical Approach to Detecting, Alerting, Monitoring and Restricting Multiple Access/Infiltration

○ Access control system combines the identification card, fingerprint recognition, and weight sensing device in a multiple manner to control unauthorized access to the restricted area.
○ Link with access control system and record the access history to the restricted area. Inspect the record on a regular basis.

○ Install the following systems in preparation of unintended situations. Install and operate the monitoring control system which offers alarms functions.
- CCTV camera and monitoring system
- Infiltration detecting system
○ Allocate security guards to perform security guarding work 24/7.

5.1.3 Matters on Physical Lock Device

Core certification system should be installed inside the security cabinet which has a physical lock device for physical access control.

5.1.4 Matters on Protection against Fire, Flood, and Power Outage

In order to prevent serious damage by unexpected power outage, SignKorea shall use an uninterruptible power supply and install a separate generator for a stable power supply.

For the protection of important systems such as the Core Certification System against flooding, SignKorea shall install them at a location where it is 30 cm or higher from the ground.

For the protection of important systems such as the Core Certification System against fire, SignKorea shall install a fire detector and use a portable fire extinguisher and automatic fire extinguisher consisting of substances that do not cause any problems on the system in time of extinguishing the fire.

5.1.5 Matters on Thermostat/Thermo-hygrostat, Ventilation, and Miscellaneous Protective Facilities

For the protection of important systems such as the Core Certification System, SignKorea installs and operates the thermostat and thermo-hygrostat to maintain temperature and humidity at a uniform level.

5.1.6 Matters on the Disposal Procedure of Facility and Equipment

SignKorea destroys its facilities and equipment when needed in a secure and physically irreparable method so that the information cannot be recovered.

5.1.7 Matters on Safe Operation of Remote Back-up Facility

SignKorea operates a remote back-up facility in a place which is at least 10-kim distant from the Accredited Certification Center of SignKorea in order to preserve important information including the accredited certificate in a remote place. The area has relevant protective facilities such as access control system and infiltration monitoring system.

5.2 Procedural Protection

5.2.1 Work Breakdown for Accredited Certification Service and Supervising Managers

SignKorea allocates accredited certificate service to a multiple number of relevant managers to secure safety and reliability of such works. The supervising managers for SignKorea's works include the followings:

○ Generation and Management of Certification (CA): CA Certification Manager, CA Policy Manager, CA Oversight Manager
○ Time Stamp Service: Time Stamp Key Manager, Time Stamp Operation Manager, Time Stamp Oversight Manager
○ Real-time Certificate Status Information (Online Certificate Status Protocol, OCSP): OCSP Operation Manager, OCSP Oversight Manager
○ Key Generation Management: Key Generation Operation Manager, Key Generation Oversight Manager, Key Generation Management Oversight Manager
○ Notices for Accredited Certification Service: Notice Operation Manager, Notice Oversight

Manager

5.2.2 Certificating Method for Accredited Certification Managers

SignKorea shall perform the process of identification for those who wish to be a truster. This process includes a face-to-face interview with a hiring manager at SignKorea or verification of identification-related documents. Further identification process shall comply with what is specified in the standing rule 5.4.1 (Requirements for Accredited Certification Service such as Personnel Qualifications and Credentials, and Identification Process).

SignKorea shall allocate accredited certificate service only to the trusters who have passed the above procedure. SignKorea shall offer or grant the corresponding personnel the following items needed for performing their allocated job.

○ Access device for entrance such as card kyes
○ Access authority to a space where access is needed
○ Digital authority such as account or password to have access to system and perform designated tasks

5.2.3 Accredited Certification Service which Cannot be Performed At Once by the Same Party

The principal rules of SignKorea's work breakdown regarding the accredited certificate service include the followings:

○ Neither CA Certification Manager, CA Policy Manager nor CA Oversight Manager can perform multiple works alone.
○ Neither Time Stamp Key Manager, Time Stamp Operation Manager nor Time Stamp Oversight Manager can perform multiple works alone.
○ Neither OCSP Operation Manager nor OCSP Oversight Manager can perform multiple works alone.
○ Neither Key Generation Operation Manager, Key Generation Oversight Manager nor Key Generation Management Oversight Manager can perform multiple works alone.
○ Neither Notice Operation Manager nor Notice Oversight Manager can perform multiple works alone.

5.3 Technical Security Control

5.3.1 Matters on Protection of Generation Key of Digital Signature

SignKorea enables access to only those persons who are permitted by the safe key generation system that is protected against physical interference without being connected to the internal and external information communication network for the generation of the pair of digital signature keys and the certificate forms.

SignKorea uses the following sizes of key and hash values for using the safe and reliable digital signature algorithm.

○ For KCDSA and RSA: 1024-bit or higher

○ For ECDSA: 160-bit or higher
○ For HAS-160 and SHA-1: 160-bit or higher

5.3.1.1 Data Storage Device

In order to safely store the generation key, SignKorea encrypts and stores data in a data storage device that has the functions such as sealing, access authorization, disclosure and alteration prevention of the generation key.

5.3.1.2 Safe Deletion Method after Generation and Use

SignKorea shall immediately delete the generation key from the system memory as soon as the generation of the generation key is completed, and shall minimize risks of external exposure when using the generation key.

5.3.1.3 Destruction Method

SignKorea shall destroy the generation key in a secure and physically irreparable method from the storage device where the applicable generation key is stored, in the event the generation key is damaged or disclosed, or the effective period of the certificate is expired.

5.3.1.4 Available Period of Pair of Digital Signature Keys

SignKorea uses a pair of digital signature keys only when the certificate of the applicable pair of digital signature key is effective.

5.3.2 Matters on System Protection such as Composition and Management of Accredited Certification System

SignKorea controls a physical and theoretic access to the system and prohibits any type of work via a remote system access. Moreover, SignKorea prescribes that the system work shall be performed by at least 2 personnel jointly.

5.3.3 Matters on Operation/Management such as Accredited Certification S/W Configuration Management

SignKorea performs tasks of managing amendments and versions of the accredited certificate S/W via its configuration management system.

5.3.4 Matters on Network Security Control such as Network Composition and Operation

SignKorea uses the infiltration prevention and detection system to manage the network in a secure manner.

5.3.5 Protection fort Management of Value-added Service such as Time Stamp Service

SignKorea uses a separate key for the OCSP and the time stamp service, and offers service via a separate system which is different from the system offering other types of services. Moreover, SignKorea maintains independence for the value-added service system by installing it in an isolated room.

5.4 Human Resources Security

5.4.1 Requirements for Accredited Certification Service such as Personnel Qualifications and Credentials, and Identification Process

SignKorea shall perform the identification process and allow only the employees with a clean slate to execute works in relation to certification and security. SignKorea shall perform human resources security for every personnel involved in the accredited certificate service including employees, partner companies, advisors and some sales representatives, system managers, designated engineers and executives who are responsible for supervising the system infrastructure of SignKorea.

The provision specified under Article 2 (Designated Standards of Accredited Certification Authority) of Enforcement Regulations of the Digital Signature Act shall apply in the qualifications and credentials of executives and employees who work for SignKorea. Those who come under Article 5 (Reasons for Disqualification) are not eligible for appointment as an executive of SignKorea.

5.4.2 Matters on Education and Duty Rotation for Accredited Certification Service

SignKorea has the operation personnel attend and complete the training session regarding the facilities for certification services, management of equipment, measures to operation, emergency reinstatement and infiltration accidents conducted by the Korea Information Security Agency pursuant to the provisions specified in Article 2 of the Enforcement Regulation of the Digital Signature Act. Furthermore, SignKorea performs an internal education pursuant to the Addendum 4 of the Provision on Protection Measures of the Accredited Certification Authority promulgated by the Ministry of Information and Communication, and the supervising managers are trained to have the managers for security, working-level engineers and employees for managing certification systems attend and complete the relevant internal and external education regarding information protection at least once a year.

5.4.3 Matters on Punishment for Unauthorized Act

SignKorea shall penalize unauthorized acts pursuant to Article 34 (Fine for Negligence) of the Digital Signature Act.

5.5 Oversight Records

5.5.1 Type and Preservation Period of Oversight Records

SignKorea shall examine any anomalies in the records regarding the operation of the accredited certificate services, and the records created by the accredited certificate system, access control system, network security system pursuant to Article 27 (Management of Oversight Records) of the Directives on Digital Signature Certification Service promulgated by the Ministry of Information and Communication. SignKorea shall preserve the following log records for at least 2 years from the date they were backed up pursuant to the Addendum 2 to 4 of the Provision on Protection Measures of the Accredited Certification Authority promulgated by the Ministry of Information and Communication.

○ Network log record
○ Oversight record regarding access records in the access control system
○ Records on actual occurrence of infiltration detection alarm
○ Records by the CCTV system

5.5.2 Protection for Oversight Records

SignKorea shall designate an employee who works for SignKorea as the oversight manager in accordance with the internal regulations for certification service, and the designated oversight manager shall review and preserve the oversight records. The oversight manager shall be the solely responsible for oversight records of the respective systems. The supervising mangers of the respective systems are allowed to view the oversight records for the corresponding services.

5.5.3 Back-up Cycle and Procedure of Oversight Records

SignKorea shall back up the records of the following certification systems with the designated intervals in the data storage devices other than the hard disk drive pursuant to the Addendum 2 to 4 of the Provision on Protection Measures of the Accredited Certification Authority promulgated by the Ministry of Information and Communication; at least once a week for the online system, and at least once a month for the offline system, other relevant system and the taped records by the CCTV system.

5.6 Preservation of Records

5.6.1 Type and Preservation Period of Records for Preservation

SignKorea shall preserve the records which regard subscribers' certificate, its suspension and revoke records for 10 years from the date when the accredited certificate concerned expired pursuant to Article 22 (Preservation of Records regarding Certification Service) of the Digital Signature Act and the Regulation on the Facilities and Equipment of the Accredited Certification Authority promulgated by the Public Administration and Security.

5.6.2 Protection of Preservation Record

SignKorea maintains security by applying the procedure control and physical access control on the preservation record and enables the inquiry on work scope. In addition, to prevent the damages and alteration of the preservation record, a thermostat and thermo-hygrostat shall be installed in the preservation place and the protective facility such as a fire alarm and other relevant facilities against the occurrence of fire.

5.6.3 Back-up Cycle and Procedure of Preservation Records

SignKorea shall make a reproduction copy against loss and destruction of the records for preservation and store them in a physically isolated and secured area. The back-up cycle shall be at least once a month.

5.7 Failback and Disaster Recovery

5.7.1 Procedure of Report/Recovery by Failure and Disaster Types in Accredited Certification Service

In the event of failure in the information processing system which provides the certification services pursuant to Article 22-3 of the Digital Signature Act, SignKorea shall immediately report the status to the Minister of Public Administration and Security or the President of Korea Information Security Agency, and come up with failback measures promptly.

The procedure of report/ recovery by disaster types shall comply with the Practical Manual for Emergency Measures in Accredited Certification Service by the Ministry of Public Administration and Security and the Korea Information Security Agency.

5.7.2 Measures for Ensured Continuity such as Failure Prevention in Accredited Certification Service

SignKorea ensures continuity of its accredited certificate service via dual system control and network dual-route control for generating/managing accredited certificates, directories, verifying the effectiveness of accredited certificate, and time stamp service.

6 Miscellaneous Matters such as Warranty in Accredited Certification Service

6.1 Warranty

6.1.1 Warranty Claim

SignKorea shall guarantee the followings are true in relation to the accredited certificate that has been issued.

○ The content contained in the issued accredited certificate is true and correct.
○ The accredited certificate was issued pursuant to the provisions of the Digital Signature Act.
○ It contains the content for suspension and revoke of the accredited certificate.

6.1.2 Exceptions

SignKorea does not guarantee matters besides what is determined by the Digital Signature Act, Enforcement Ordinance and Enforcement Regulations of the same act, or the ‘6.1.1 Warranty Claim’ of this statement; in other words, SignKorea does not guarantee credibility of the subscriber and invariability of the information that regards the subscriber, and so on.

6.2 Compensation

6.2.1 Limitation and Immunity of Compensation

SignKorea is designated by the government and equipped with financial capability in performing the certification service, and is subscribed to insurance in response to damages by the work mistake and negligence of SignKorea for subscriber and user pursuant to Article 26 (Compensation Responsibility) of the Digital Signature Act.

SignKorea may make compensation to a subscriber or user who has proven the cause of compensation in the event loss or damage occurs by the cause of certificate or certification service of SignKorea regardless of the grade of certificate. However, SignKorea shall not make compensation on the part that exceeds the total amount of compensation (KRW 5 billion) from the insurance that SignKorea subscribed. On the loss that exceeds the total amount of compensation of SignKorea, a subscriber or user may enter into the agreement of a separate rate following the selection of subscriber or user.

The limit of such a damage compensation is applied to all types of damages and losses occurring by trusting the certification for a certificate subscriber or user. The total amount of compensation of each certificate is KRW 4 billion for accredited certificate for Platinum service, KRW 5 billion for accredited certificate for servers, and KRW 2.5 billion for accredited certificate for other use. In the event that the demand for compensation exceeds the total amount of compensation, SignKorea shall make compensation first in the order that the compensation request in writing is received after finally resolving the dispute unless there is an order by the court decision.

SignKorea shall not be held accountable for the delay or inability to process the certification service occurring by external factors (for example: war, natural calamities, power outage, fire and other external factors) which are impossible to be controlled by SignKorea.

6.2.2 Scope of Compensation Coverage

The insurance that SignKorea has insured puts up SignKorea and the Registration Agency which has concluded an agreement with SignKorea as security.

6.3 Dispute Resolution

6.3.1 Requirements for the document (or digital document) delivered to the party concerned with the Digital Signature Certification Scheme to hold legal effect.

In order for the document (or digital document) delivered to the party concerned with the Digital Signature Certification Scheme to hold legal effect, it should satisfy the following requirements.

○ The document should include the digital signature based on the accredited certificate, and the

digital signature should satisfy the following conditions:
- The digital signature generation information regarding the digital signature should be exclusive to the subscriber; the subscriber should control and manage the digital signature generation information at the point of signing it; the updated status of the digital signature concerned after the digital signature was created should be able to be easily checked; the updated status of the digital document concerned after the digital signature was created should be able to be easily checked.

○ The accredited certificate used for the digital signature should be valid; it should not be in the status of suspension or revoke.

6.3.2 Governing Law on Interpretation and Execution of Standing Rule

This Rule shall be interpreted and applied in accordance with the Digital Signature Act of Korea and the relevant ordinances.

6.3.3 Court of Jurisdiction for Lawsuits

In order to settle a dispute arising between SignKorea and subscriber, or SignKorea and the trustee regarding the certification service, SignKorea shall designate the courthouse where the principle place of business for SignKorea is located as the court of jurisdiction.

6.3.4 Dispute Settlement Procedure regarding Certification Service

In the event that a dispute arises out of SignKorea's certification service, the relevant authorities such as the Ministry of Public Administration and Security shall investigate whether SignKorea has engaged in any act of violation in relation to the Digital Signature Act, and settle disputes in a prompt manner in accordance with the Digital Signature Act and the relevant legal procedure.

6.4 Privacy Protection

SignKorea has devised the privacy policy based on the [Act on Promotion of Information and Communication Network Utilization] which engages in the scope of protection and accountability for the information in relation to the accredited certificate service and complies with it. Our Privacy Policy is posted on the URL address below.

○ URL address for Privacy Policy of SignKorea: http://www.signkorea.com/privacy.html

6.5 Oversight and Inspection, and others

The Ministry of Public Administration and Security and the Korea Information Security Agency perform a regular inspection for the accredited certificate institutions once every year to inspect overall matters such as the accredited certificate service, system H/W, S/W and protection facilities, and SignKorea complies with it in good faith. Moreover, SignKorea goes through a substantial examination by the Ministry of Public Administration and Security and the Korea Information Security Agency every time a change arises in the services and systems for accredited certificate.

6.6 Compliance with Relevant Laws

Parties concerned with the Digital Signature Certification Scheme should comply with the law of the Republic of Korea and the relevant ordinances.

6.7 Validity of the Certification Practice Statement

6.7.1 Implementation Date of the Certification Practice Statement

The newly-established or revised standing rule shall be implemented from the day when SignKorea posts it in the location for data storage.

6.7.2 Cessation in Validity of the Certification Practice Statement

This standing rule shall be considered no longer valid in the event that it is replaced with the revised standing rule.