CrossCert
Licensed Certification Authority

Certification Practice Statement

Version 2.1

CROSSCERT: Korea Electronic Certification Authority, Inc.

This Certification Practice Statement prescribes the general procedures and matters regarding the usage and operation of the authorized certification work and services of CrossCert which is the designee as the licensed certification authority by the Ministry of Public Administration and Security. This Certification Practice Statement complies with the Digital Signature Act, its enforcement decree and enforcement rule and the certification practice statement of Korea Internet & Security Agency.

Table of Contents

5.1.2 Controlling Physical Access
5.1.3 Prevention of Fire, Water Exposure, Power Failure and Protection etc.
5.1.4 Equipment and Facility Disposal Procedure
5.1.5 Safe Operation of Back-Up Facility Located in Remote Place

5.2 Procedural Protective Measures
5.2.1 Task Allocation and Responsible Personnel on Licensed Certification Work
5.2.2 Verification Methods on Responsible Personnel of Licensed Certification Work
5.2.3 Licensed Certification Work Which Can Not be Performed Simultaneously by the Same Person

5.3 Technical Protective Measures
5.3.1 Issues Regarding Protection of Digital Signature Creating Key
5.3.2 Issues Regarding Protection for Composition and Management of Licensed Certification System etc.
5.3.3 Issues Regarding Configuration Management of Licensed Certification Software etc.
5.3.4 Issues Regarding Protection for Composition and Operation of Network etc.
5.3.5 Protective Measures on Additional Services including Time-Stamping etc.

5.4 Personnel Security
5.4.1 Qualifications, Experience etc Requirements and Background Check Procedures on Responsible Personnel of Licensed Certification Work
5.4.2 Training Licensed Certification Work and Job Rotation
5.4.3 Sanctions for Unauthorized Actions

5.5 Audit Record
5.5.1 Types of Audited Records and Retention Period
5.5.2 Protective Measures, Back-Up Period, and Procedure for Audited Records

5.6 Records Archival
5.6.1 Types of Records Archived and Retention Period
5.6.2 Protective Measures on Records Archived
5.6.3 Back-Up Period and Procedure for Records Archived

5.7 Failure Restoration and Disaster Recovery
5.7.1 Report and Recovery Procedure upon the Occurrence of Impediments and Disastrous Incidents on Licensed Certification Work
5.7.2 Assuring Plan for Continuity Capabilities including Prevention of Occurrence of Obstacles to

Licensed Certification Work

Chapter 6. Warranties on Licensed Certification Work etc., Miscellaneous Matters

6.1 Warranties
6.1.1 Warranties on Licensed Certification Work and Disclaimers of Warranties

6.2 Liability
6.2.1 Compensation Policy in Relation to Licensed Certification Service
6.2.2 Limitations of Liability by the Insurance CrossCert subscribed
6.2.3 Indemnities

6.3 Dispute Resolution
6.3.1 Requirements for Having Legal Validity on the Document Transmitted to a Relevant Party of Digital Signature Certification System
6.3.2 Interpretation of Certification Practice Statement and Governing Law in Relation to Enforcement
6.3.3 Competent Court for Legal Proceedings
6.3.4 Dispute Resolution Procedure

6.4 Privacy of Personal Information
6.4.1 Policy on Privacy of Personal Information

6.5 Inspection and Check-up etc.

6.6 Compliance with Applicable Law

6.7 Effectiveness of Certification Practice Statement
6.7.1 Effective Date
6.7.2 Conditions for Termination of Certification Practice Statement

Chapter 1. Overview

1.1 Background and Objective

1.1.1 Background and Objective of Certification Practice Statement

Korea Electronic Certification Authority, Inc. (hereinafter, "CrossCert") which is designated as a licensed certification authority, establishes this Certification Practice Statement in order to define necessary matters for the licensed certification work and certification system and procedures thereof, including the issuance (new issuance/renewal/re-issuance) of an authorized certificate, suspension and recovery of its validity, revocation etc. and to prescribe the responsibilities and obligations in relation to the certification work. CrossCert's Certification Practice Statement deals with the general process from the establishment and commencement of the licensed certification center, operating records archives to registration of the applicants.

1.1.2 Introduction of Digital Signature Certification System

Authorized Digital Signature Certification System (hereinafter, "Certification System") means the system for providing the works on the issuance of authorized certificates and management of records related to the certification and the additional works by using the authorized certificates etc.

1.1.3 Introduction of CrossCert

CrossCert is the first privately owned certification company in Korea which was found on 15 March 1999 as the brand of "CrossCert" for the purpose of performing international reciprocal certification service through the retention of the international certification technology and public confidence. CrossCert has provided the licensed certification service (hereinafter, "Certification Service") on the basis of Public Key Infrastructure according to Digital Signature Act (hereinafter, "Act") in order to provide the licensed certification service since it has been designated as an licensed certification authority from the Ministry of Public Administration and Security on 24 November 2001 according to Article 4 (Designation of Licensed Certification Authority) of the Act. The contact information in relation to the Certification Service is as the followings.

Name of Organization	Licensed Certification Center of Korea Electronic Certification Authority Inc.

	(English Name: CROSSCERT: Korea Electronic Certification Authority, Inc.)
Address	7th Floor, Halim Building 1674-4 Seocho-Dong, Seocho-Gu SEOUL
URL	http://www.crosscert.com/
Electronic Mail	helpdesk@crosscert.com
Telephone Number	1566-0566
Fax Number	02)3019-5656

1.1.4 Definition and Validity of Authorized Certificate

Authorized Certificate means a certificate issued by a licensed certification authority according to Article 15 (Issuance of Authorized Certificate) of the Act out of the certificates that are the electronic information proving and checking the fact that the digital signature creating information is uniquely belonged to the subscriber etc.

If there exists an authorized digital signature on the basis of an authorized certificate, it shall be assumed that such digital signature is the sign or/and seal of the signatory and that electronic document is not changed in its contents.

1.2 Name of Certification Practice Statement

This Certification Practice Statement is version 2.1 of CrossCert's Certification Practice Statement.

1.3 Parties Engaged in the Digital Signature Certification System

1.3.1 Ministry of Public Administration and Security

Ministry of Public Administration and Security is a policy making and supervisory authority for the system building the environments for using digital signatures safely and trustfully and managing the licensed certification authority effectively (hereinafter, "Certification Management System"). Further it performs the following duties.

- Designation of Licensed Certification Authority, Issuance of Corrective Order and Suspension of Work, Cancellation of Designation, and Investigation on Work
- Management and Supervision Whether Licensed Certification Authorities comply with the relevant laws on Digital Signature Act

- Policy Making in order to establish and operate the safe and reliable certification management system
- Mutual Recognition of Digital Signatures with Foreign Governments

1.3.2 Korea Internet & Security Agency

Korea Internet & Security Agency performs the following duties as the highest certification authority in accordance with Article 8 (Performance of Certification Work by Licensed Certification Authority), Article 10 (Cessation, Closure, etc. of Certification Work), Article 12 (Suspension of Certification Work and Revocation of Designation, etc.), and Article 25 (Digital Signature Certification Control Service) of the Act.

- Substantive Assessment for Designation of Licensed Certification Authority
- Inspection and Supports for Safe Operation of Licensed Certification Authority
- Performing Certification Work including Certification on Digital Signature Verifying Key of Licensed Certification Authority etc.
- Establishment and Operation of Mutual Recognition System
- Establishment and Operation of Safe Certification Management System
- Taking Over the Subscribers Authorized Certificates etc. of Licensed Certification Authority Who Revoked its Certification Work
- Development and Distribution of Certification Technology of Digital Signature
- Taking Over the Subscribers Authorized Certificates etc. of Licensed Certification Authority Who Has Been Cancelled its Designation
- Other Relevant Works in association with Digital Signature

1.3.3 CrossCert

1.3.3.1 Role

CrossCert performs the following duties as a licensed certification authority in accordance with Article 4 (Designation of Licensed Certification Authority) and Article 8 (Performance of Certification Work by Licensed Certification Authority) of the Act.

- Verifying the Identity of Subscriber
- Receipt and Process all the relevant application documents related to Certification Service
- Designation, Operation and Management of Registration Authority
- Providing Time-Stamping Service
- Providing Certification Service, Including Issuance(New/Re-Issuance/Renewal), Suspension,

Recovery, Revocation etc. of Authorized Certificate

- Making Public Notification of Information on Lists, Suspension and Revocation Lists, etc of Authorized Certificate
- Making Public Notification of Certification Practice Statement
- Making Public Notification of Information regarding Authorized Certificate
- Other Relevant Works in association with Certification Service

1.3.3.2 Responsibility and Obligation

① Compliance with Relevant Laws and Certification Practice Statement

CrossCert complies with the related laws to digital signatures and Certification Practice Statement of Korea Internet & Security Agency while it performs and provides Certification Service.

② Providing Information Relevant to Licensed Certification Authority

CrossCert has the obligation and responsibility to provide the accurate information and facts to Korea Internet & Security Agency in relation to the following matters.

- Substantive Assessment on Designation of Licensed Certification Authority
- Application for Issuance(New/Re-Issuance/Renewal) of Authorized Certificate for the use of Licensed Certification Authority
- Application for Suspension and Revocation of Authorized Certificate for the use of Licensed Certification Authority
- Application for Validity Recovery etc of Authorized Certificate for the use of Licensed Certification Authority

CrossCert has the obligation and responsibility to make public notification without delay on the following matters that may affect the credibility and validity of authorized certificate to its subscribers and users.

- Cessation, Discontinuance or Closure of Certification Work of Licensed Certification Authority
- Cancellation of Designation for Licensed Certification Authority
- Transfer or Merger of Licensed Certification Authority
- Information regarding Authorized Certificate
  - Subscriber's Authorized Certificate
  - Suspension and Revocation List etc of Subscriber's Authorized Certificate
- Other Information relevant to Performance of Certification Work etc

CrossCert publicly notifies the information relevant to a licensed certification authority through its

web-site. Further CrossCert provides the directory service that allows you to search the status of authorized certificate, including the information on authorized certificate, its suspension and revocation list etc. through the information networks at any time.

③ Providing Certification Service

CrossCert shall not deny providing certification services without a justifiable reason and it shall not unfairly discriminate subscribers or users. CrossCert provides the following certification services to subscribers and users.

- Issuance(New/Re-Issuance/Renewal) of Authorized Certificate
- Suspension, Recovery, Revocation of Authorized Certificate
- Verifying the Identity in relation to Providing Authorized Certification Services (Issuance, Suspension, Recovery, Revocation etc.)
- Making Public Notification of Information regarding Authorized Certificate
- Other Relevant Service etc. in association with Authorized Certificate

④ Guarantee of Certification Service

CrossCert guarantees the followings to the subscriber's authorized certificate that issued by the digital signature creating key which is matching the digital signature verifying key included in the authorized certificate for the use of licensed certification authority issued from Korea Internet & Security Agency for CrossCert.

- The Fact that there is no difference between the contents of the issued authorized certificate and that of the applied & registered facts
- The fact that there is no incorrect contents regarding the authorized certificate suspension and revocation list
- The fact that the authorized certificate is issued in compliance with the Digital Signature Act and Certification Practice Statement

However it does not mean that the authorized certificate guarantees other than the above-mentioned matters, including the credit ratings of subscriber and user, invariability of subscriber's information etc.

⑤ Protecting Subscriber's Private Information and Maintaining Security of Records

CrossCert protects subscriber's private information and maintains security of records in compliance with the Policy on Privacy of Personal Information prescribed in 6.4.1 of this Certification Practice Statement.

⑥ Proper Use of Digital Signature Creating Key

CrossCert can generate the following various digital signature creating keys according to its purpose of use. However, the digital signature creating key is only available to use in the field that it was initially intended to being used.

- Digital Signature Creating Key for Authorized Certificate Issuance: Only Used in Issuing Authorized Certificate
- Digital Signature Creating Key for Time-Stamping: Only Used in Time-Stamping
- Digital Signature Creating Key for Online Certificate Status Protocol (OCSP): Only Used in OCSP
- Other Digital Signature Creating Key: Only Used in the Relevant Purpose

⑦ Protection of Digital Signature Creating Key

CrossCert generates its digital signature creating key for the use of licensed certification authority in a safe manner by using the reliable software and hardware etc and further it manages safely in order to prevent from loss, damage, or being stolen or leaked of the generated digital signature creating key.

⑧ Reporting and Taking Measures on Important Facts

CrossCert reports the following important facts when it occurs to Ministry of Public Administration and Security and Korea Internet & Security Agency without delay and it takes the legal measures according to Article 6 (Report on Assignment and Merger) and Article 7 (Report on Cessation etc of Certification Work) of the Enforcement Decree.

- When the facts that materially affect to the credibility and validity of authorized certificate occurs, including the damage, exposure, break-out, loss, being stolen etc of the creating key according to Article 21 (Control of Digital Signature Creating Key) of the Act
- When the circumstances that materially affect certification works of CrossCert occurs according to Article 9 (Acquisition of Certification Work by Transfer, etc.), Article 10 (Cessation, Closure, etc. of Certification Work), Article 12 (Suspension of Certification Work or Revocation of Designation, etc.) and Article 27 (Protection of Subscribers and Users) etc.

In addition, it is the principle that the occurrence of the above-mentioned facts shall be notified without delay through the web-site of CrossCert.

1.3.4 Registration Authorities

1.3.4.1 Role

CrossCert may designate and operate a juristic person who performs the verification work on subscriber's identity and receiving & registering the applications for the issuance, suspension, recovery, or revocation of authorized certificate on behalf of CrossCert (hereinafter, "Registration Authority"). Duties of Registration Authority are the followings.

- Receiving and Registering the Application for Issuance(New/Re-Issuance/Renewal), Suspension, Recovery, Revocation of Authorized Certificate
- Verifying the Identity of the Applicant for Certification Service
- Other Work Assigned by CrossCert in Relation to Certification Service

1.3.4.2 Responsibility and Obligation

① Acknowledgement of Certification Practice Statement

Registration Authority shall comply with CrossCert's Certification Practice Statement and the agreement made with CrossCert and it owes the responsibility for the accuracy of the verification of the identity of subscribers.

② Verification of Subscriber's Identity

Registration Authority shall verify the identity of the applicant who intends to be issued the authorized certificate according to the requirements and methods for verification of identity as provided in Article 13.2 of Enforcement Rule of the Act and confirm the integrity of the relevant contents of the application.

③ Compensation and Liability

Registration Authority shall be responsible for the damages occurred to subscriber or user due to its non-compliance with the obligations under this Certification Practice Statement.

④ Compliance with Certification Practice Statement

Registration Authority shall have the obligation to perform its duties prescribed in this Certification Practice Statement in good faith in relation to providing the Certification Service.

⑤ Protection of Subscriber's Private Information

Registration Authority shall have the obligation to protect the subscriber's private information that is acquired from the performance of its registration work and to keep the security for the records.

1.3.5 Transmission Service Provider

1.3.5.1 Role

Transmitting Service Provider is a juristic person who operates the system transmitting subscriber's registered information etc. (hereinafter, "Transmitting System") after entering into agreements between CrossCert and Registration Authority.

1.3.5.2 Responsibility and Obligation

① Acknowledgement of Certification Practice Statement

Transmitting Service Provider shall acknowledge CrossCert's Certification Practice Statement and it shall be obligated to comply with the contents of the agreement made with CrossCert, further to transmit the following information as they were initially transmitted from CrossCert and Registration Authority.

- Subscriber's Name(Name of Individual or Corporation), Identification Number(Residence Registration Number or Business Registration Number etc), Address, Telephone Number, Email Address, Distinguished Name(DN) etc, Subscriber's Registered Information
- Reference Number and Approval Code Generated by CrossCert

② Transmission Service Provider's Obligation

Transmission Service Provider shall equip the Transmitting System and protective facilities according to Notification [Rules on Protective Measures of Licensed Certification Authority] of Ministry of Public Administration and Security as to the following matters.

- Controlling Access
- Monitoring Physical Invasion
- Protecting System and Network

In addition, it shall report the establishment and change of Transmitting System whenever it happens to the Minister of Public Administration and Security and it shall record and maintain the storage for the change of the Transmitting System and protective facilities, further it shall receive the periodic inspection on the stability of the system and operation in general in relation to transmission service more than once a year by Korea Internet & Security Agency.

③ Compensation and Liability

Transmission Service Provider shall be responsible for the damages occurred to CrossCert, subscriber or user due to its non-compliance with the obligations under this Certification Practice Statement.

④ Compliance with Certification Practice Statement

Transmission Service Provider shall have the obligation to perform its duties prescribed in this Certification Practice Statement in good faith in relation to providing the Certification Service.

⑤ Protection of Subscriber's Private Information

Transmission Service Provider shall have the obligation to protect transmitted subscriber's private information and to keep the security for the records.

1.3.6 Subscriber

1.3.6.1 Role

Subscriber means a person whose digital signature creating information has been certified by CrossCert.

1.3.6.2 Responsibility and Obligation

① Providing Accurate Information

Subscriber shall apply an authorized certificate by selecting upon his/her purpose to use and have obligation to provide the accurate information and facts to CrossCert in the following cases.

- When Applies Issuance(New/Re-Issuance/Renewal) of Authorized Certificate
- When Applies Suspension of Authorized Certificate
- When Applies Recovery from Suspension of Authorized Certificate
- When Applies Revocation of Authorized Certificate
- When Providing Changed Information of Subscriber in the Application for Change of Personal Information

② Management of Digital Signature Creating Information

Subscriber shall store and retain his/her digital signature creating information in a safe manner and he/she shall notifies the facts when he/she becomes aware of the risks of loss, damage or being stolen, leaked of the afore-mentioned information to CrossCert. In this case, subscriber shall notify users the contents as reported to CrossCert.

③ Management of Authorized Certificate

Subscriber shall exercise precautions in preserving the accuracy and integrity of the written items in the authorized certificate or information relevant to the authorized certificate during the

effective period of authorized certificate. In addition, subscriber shall not unlawfully use the authorized certificate out of its scope of use or its purpose, nor assign or lend the authorized certificate to other person for making it available to their use, nor being assigned or borrowed from other person for subscriber's use.

④ Subscriber's Compensation and Liability

Subscriber shall be responsible for the damages occurred to CrossCert or user due to its non-compliance with the obligations under this Certification Practice Statement.

1.3.7 User

1.3.7.1 Role

User means a person who uses an authorized certificate issued by CrossCert.

1.3.7.2 Responsibility and Obligation

① Matters to Be Observed by User

User shall take the following measures in order to ascertain the authenticity of the authorized digital signature by (1) subscriber's name (2) digital signature verifying information (3) digital signature methods used by CrossCert (4) serial no. of authorized certificate (5) expiry date of authorized certificate (6) information confirming that CrossCert is the licensed certification authority.

- Confirming Whether Authorized Certificate is Valid
- Confirming Whether Authorized Certificate is Suspended or Revoked
- Confirming the Relevant Matters If Authorized Certificate is Being Limited the Scope of its Use or its Purpose
- Confirming the Relevant Matters If Subscriber Has a Power of Attorney on behalf of a Third Person or It Has been Requested for Indication of Professional Qualifications etc.

② Prohibition of Demanding Certain Authorized Certificate

User shall not specifically request for an authorized certificate issued by identifying a specific licensed certification authority without a justifiable reason when it is confirming the digital signature by using an authorized certificate.

③ User's Compensation and Liability

User shall be responsible for the damages occurred to CrossCert or subscriber due to the unlawful conducts resulted from his/her willful misconduct or negligence.

1.4 Management of Certification Practice Statement

1.4.1 Responsible Department and Contact Information of Certification Practice Statement

The management of this Certification Practice Statement is in charge of Management Planning Department of CrossCert and the contact information is as the followings.
(Tel: 02-3019-5563 Fax: 02-3019-5656 Email: cps@crosscert.com)

1.4.2 Reasons for Amendment of Certification Practice Statement

CrossCert amends Certification Practice Statement when one of the following events occurs.

- If the Minister of Public Administration and Security orders the amendment of this Certification Practice Statement in accordance with Article 6.2 of the Act
- If the contents or procedure for CrossCert's Certification Service is changed or it is determined that the change of Certification Practice Statement is necessary due to the introduction of new services related to certification, Certification Practice Statement may be amended.

1.4.3 Establishment and Amendment of Certification Practice Statement

1.4.3.1 Reports on Establishment and Amendment of Certification Practice Statement

CrossCert reports the Certification Practice Statement amended or established according to Article 6 (Rules, etc. of Authorized Certification Work) of the Act to the Minister of Public Administration and Security until 15 days before it performs the certification work according to the amended Certification Practice Statement.

1.4.3.2 Public Notification of Certification Practice Statement

CrossCert notifies the established or amended Certification Practice Statement through the URL allocated in the site for the storage of information related to authorized certificates 2 weeks prior to the commencement of its application. The public notification is made by uploading into CrossCert's web site (http://gca.crosscert.com).

CrossCert may, at its discretion, change all or part of Certification Practice Statement if it regards

necessary. In this case, CrossCert notifies the changed Certification Practice Statement 2 weeks prior to the commencement of its application and notifies subscriber the change of the Certification Practice Statement.

1.4.3.3 Methods for Acquiring Subscriber's Consent on the Amendment of Certification Practice Statement

The changed Certification Practice Statement shall be regarded as 'consented' by subscriber if subscriber does not raise any objection on the changed Certification Practice Statement within 2 weeks from the notification made by phone, letter, or email, which CrossCert shall notifies the foregoing contents of 'regarded as consent' upon the notification of the changed Certification Practice Statement. Notification may be made by the same ways of announcement or emailing.

1.5 Definitions and Acronyms

Distinguished Name(DN): Form of names complying with the X.500 Standard and being used in order to ascertain the Issuer and holder of authorized certificate.

Directory: System complying with the X.500 Standard for providing notice and search services to a reliable party and storing authorized certificate and its suspension and revocation lists.

Service Disruptive Attack: Attacking activity disrupting the usual functioning of system.

Real Name: Name under the Residence Registration, name under the business registration, other substantive name defined under Act on Real Name Financial Transactions and Guarantee of Secrecy and its Enforcement Decree.

Certification: The act of ascertaining and verifying the fact that digital signature verifying key is matching to the digital signature creating key owned by a person or a corporation.

Electronic Document: Information prepared, transmitted, received or stored in the electronic form by the information processing system, computer etc.

Digital Signature: Generated information from digital signature creating key by using the asymmetric cryptosystem which is enabling to verify the identity of the writer of the electronic document and whether the contents of the electronic document is changed, which is unique to the electronic document.

Digital Signature Verifying Key: Electronic information used for verifying a digital signature.

Digital Signature Creating Key: Electronic information used for creating a digital signature.

Digital Signature Key: Digital signature creating key and its matching digital signature verifying key.

Core Certification System: Key creating system, generation and management system for authorized certificate, directory system and time-stamping system.

Chapter 2. Types of Authorized Certificates and Fees

2.1 Types of Authorized Certificates

CrossCert issues authorized certificates for individuals and corporations. Types, objects of issuance, purpose and validity period of the issued authorized certificates are as the followings.

Type of Authorized Certificate		Object of Issuance	Purpose (Scope of Use)	Validity Period	Remarks
Wired Service	General	Corporate/Organization, Self-Employed	General Electronic Transaction, Electronic Bidding	1 Year	
		Individual(Inter-working)	General Electronic Transaction	1 Year	
		Individual(Inter-working, Premium)	General Electronic Transaction	1 Year	
		Server(for Hard Coding)	General Electronic Transaction	1 Year	Authorized Certificate loading server for digital signatures
	Specific	Corporate/Organization, Self-Employed, Individual	Specific Transactions, Specific Purposes	1 Year	
Wireless Service		Individual, Corporate/Organization, Self-Employed	Wireless Electronic Transactions	1 Year	

[Table 1] Types and Uses etc of Authorized Certificates

❑ Despite the above table, the validity period is subject to change upon the customer's credit

ratings, for example it may be issued by adjusting as 'less than 1 year' or 'more than 1 year' of period.

2.2 Fees for Authorized Certification Service

Type of Certificate		Object of Issuance	Fees (Unit: Won, VAT included)	Remarks
Wired Service	General Purpose	Corporate/Organization, Self-Employed	110,000	
		Individual (Inter-working)	4,400	
		Individual (Inter-working Premium)	11,000	
		Server(for Hard Coding)	1,100,000	
	Specific Purpose	Corporate/Organization, Self-Employed, Individual	To be agreed by separate agreement	
Wireless Service		Individual	13,200	
		Corporate/Organization, Self-Employed	110,000	

- The above fees for the use of one year and the validity period of authorized certificateshall be decided within the maximum validity period for each authorized certificate, subsequently the amount of the fees shall be increased in proportion to the validity period.

[Table 2] Fees for Authorized Certificates

- Fees for Access to Authorized Certificates: No fees will be imposed to a user who access to and confirm an authorized certificate.
- Fees for Access to Revocation of Authorized Certificate and its Status Information: No fees will be imposed to a user who access to revocation of Authorized Certificate and its status information.
- Fees for Other Services: Fees may be imposed in relation to other services if it is regarded as necessary.

2.3 Refund

2.3.1 Refund Policy on Authorized Certification Service

Subscriber may request for and receive the refund of fees by visiting Registration Authority that she/he initially applied (1) within 20 days from the expiry date for issuable period (i.e. 14 days) of authorized certificate as prescribed in 3.1.2 of this Certification Practice Statement if an authorized certificate is not issued, (2) within 7 days from the issuance date if an authorized certificate is

issued. If there incurred necessary expenses for the issuance of an authorized certificate, the fees may be refunded after the deduction of the expenses is made and the details of the foregoing shall be notified to the subscriber when the refund is made.

Chapter 3. Issuance of Authorized Certificate etc., Authorized Certification Work

3.1 Application for Issuance of Authorized Certificate

3.1.1 Filing Application for Authorized Certificate Issuance

The subjects of the application for an authorized certificate are individual, corporation or organization and the application subject, in person or through its representative, applies by submitting the application document for authorized certificate issuance according to this section to CrossCert or Registration Authority.

3.1.1.1 Authorized Certificate for Individuals

- Individual (Majority)
  - Application Form of Authorized Certificate
  - Resident Registration Card if s/he is an eligible person to being issued the card
  - Provided if it is difficult to use a resident registration card, a copy of proof issued by the national or a local government authority and/or school principal according to the education laws that may verify the identity by indicated name, residence registration no. and affixed his/her photograph (original copy should be presented)
- Minority
  - When Minority Applies Independently
    - Application Form of Authorized Certificate
    - Resident Registration Card (a copy of proof issued by the national or a local government authority and/or school principal according to the education laws that may verify the identity by indicated name, residence registration no. and affixed his/her photograph)
    - Consent Letter of Legal Representative(Personal Seal Impression should be stamped)
    - Seal Impression Certificate of Legal Representative
  - When Minority Applies with Legal Representative
    - Application Form of Authorized Certificate
    - Resident Registration Card (a copy of proof issued by the national or a local

government authority and/or school principal according to the education laws that may verify the identity by indicated name, residence registration no. and affixed his/her photograph)

- Copy of Resident Registration if s/he is not eligible to being issued the card
- Identification Certificate of Legal Representative

☐ Overseas Residents

- Application Form of Authorized Certificate
- One Copy out of Passport and Overseas Resident Registration Card (original copy should be presented)

☐ Foreigners

- Application Form of Authorized Certificate
- One Copy out of Passport, International Driver's License, Seaman's Pocket Ledger, or Foreigner Registration Card according to the Immigration Control Act (original copy should be presented)
- Copy of Identity Proving Document Issued by the Individual's National Authority if there is no above-mentioned proof and the foreigner registration card is not issued (original copy should be presented)

3.1.1.2 Authorized Certificate for Corporations

① When the representative of a corporation applies for the issuance of an authorized certificate by visiting in person to CrossCert or Registration Authority.

☐ Domestic Corporation

- Application Form of Authorized Certificate
- Proof of Verifying the Identity of Corporation
  - ☐ One copy out of Company Register, Commerce Register according to the Non-Contentious Case Litigation Procedure Act, Business Registration Certificate according to the Corporate Tax Act, Payment of Tax Certificate according to the Income Tax Act, Identification Number Certificate according to the Value Added Tax Act, and Certificate for Business Registration (In case of Company Register or Commerce Register, the original copy should be submitted.)
- One copy of the representative's resident registration card, passport , driver's license or a certificate issued by a national authority or head of a local authority with affixing a photograph thereon (Original copy should be presented.)

☐ Organization

- Application Form of Authorized Certificate
- Proof of Verifying the Identity of Organization
  - If Tax Payment No. or Reference No. exists: Copy of Notification Letter stating the grant of Tax Payment No. or Reference No. (Original copy should be presented.)
  - If there is no Tax Payment No. or Reference No.: One copy of the representative's resident registration card, passport , driver's license or a certificate issued by a national authority or head of a local authority with affixing a photograph thereon (Original copy should be presented.)

- Foreign Corporation or Foreign Organization
  - Application Form of Authorized Certificate
  - Proof of Verifying the Identity of Corporation/Organization
    - Copy of Company Register (or Commerce Register) issued by relevant authority of its country or a certificate ascertained by the relevant authority of its country or the embassy exists in Korea proving the existence of the Corporation/Organization etc. (Original copy should be presented.)
  - Copy of the Representative's Identification Certificate (Photograph affixed) (Original copy should be presented.)

- Self-Employed
  - Domestic Residents
    - Application Form of Authorized Certificate
    - Copy of Self-employed Business Registration Certificate
    - One copy of the representative's resident registration card, passport , driver's license or a certificate issued by a national authority or head of a local authority with affixing a photograph thereon (Original copy should be presented.)
  - Overseas Residents
    - Application Form of Authorized Certificate
    - Copy of Business Registration Certificate
    - Copy of the Representative's Passport or Overseas Resident Registration Card (Original copy should be presented.)
  - Foreigners
    - Application Form of Authorized Certificate
    - Copy of certificate issued by the country's national authority with proving that it has been established in its country (Original copy should be presented.)
    - Copy of the Representative's Identification Certificate (Photograph affixed) (Original copy should be presented.)

② If an agent applies for the issuance of an authorized certificate by visiting to CrossCert or Registration Authority, 3.1.1.4 of this Certification Practice Statement shall be applied.

3.1.1.3 Server Authorized Certificate

① When the representative applies for the issuance of an authorized certificate by visiting in person to CrossCert or Registration Authority.

Necessary documents for the application of server authorized certificate are as the followings. Provided a foreign corporation and foreign organization, foreign business person should submit the documents as indicated in 3.1.1.2 (Authorized Certificate for Corporations) hereof.

☐ Server Authorized Certificate for Corporation

- Application Form of Authorized Certificate
- Proof of Verifying the Identity of Corporation
  - One copy out of Company Register, Commerce Register according to the Non-Contentious Case Litigation Procedure Act, Business Registration Certificate according to the Corporate Tax Act, Payment of Tax Certificate according to the Income Tax Act, Identification Number Certificate according to the Value Added Tax Act, and Certificate for Business Registration (In case of Company Register or Commerce Register, the original copy should be submitted.)
- One copy of the representative's resident registration card, passport , driver's license or a certificate issued by a national authority or head of a local authority with affixing a photograph thereon (Original copy should be presented.)
- URL registration proving documents issued by a URL registration authority

☐ Server Authorized Certificate for Self-Employed

- Application Form of Authorized Certificate
- Copy of Self-employed Business Registration Certificate
- One copy of the representative's resident registration card, passport , driver's license or a certificate issued by a national authority or head of a local authority with affixing a photograph thereon (Original copy should be presented.)
- URL registration proving documents issued by a URL registration authority

② If an agent applies for the issuance of an authorized certificate by visiting to CrossCert or Registration Authority, 3.1.1.4 of this Certification Practice Statement shall be applied.

3.1.1.4 When an Agent Applies

When an authorized certificate or a server authorized certificate is applied, the verification of the representative's identity may be replaced by verifying the officer or employees of the corporation who has been duly authorized from the representative. In this case the following additional documents are necessary.

- Application Form of Authorized Certification Service
- Identity Verification Proof as prescribed in 3.1.1.2 hereof.
- Power of Attorney (Seal Stamped)
- Corporation's Seal Impression Certificate (Representative's Seal Impression Certificate in case of Self-employed)
- Copy of the Agent's Identity Verification Certificate (Original Copy should be presented.)

3.1.2 Available Period for Issuance of Authorized Certificate

If the creation of an authorized certificate is not requested within maximum 14 days (including holidays etc.) from the application date after the application made to Registration Authority or CrossCert, the application for the subscription of an authorized certificate becomes invalid.

3.1.3 Issuance Procedure and Its Requirements

① Issuance Procedure

CrossCert issues an authorized certificate when a subscriber requests for the creation of an authorized certificate after inputting a reference number and a approval code with connecting to CrossCert's Authorized Certificate Issuance System after the receipt of a reference number and a approval code from a registration authority.

② If the Issuance Application is Rejected

CrossCert may reject the issuance application for authorized certificates if one of the following reasons comes out.

- Application under the name of others
- Application made with providing false information on the application form or attaching the false document
- Payment of certification fees has not been made within the due date as prescribed in Certification Practice Statement
- It becomes impossible or impracticable to verify the applicant's identity by the submitted documents
- Breach of other laws and regulations or application of authorized certificate issuance for the improper purpose

CrossCert may reject the issuance of an authorized certificate if it discovers the foregoing reasons at any time before issuing an authorized certificate even after the application has been made.

3.1.4 Verification Items of Subscriber Information

CrossCert and Registration Authority shall ascertain the following items of the applicant on the basis of its real name in order to verify the authenticity of the subscriber's information.

- Individual
  - ① Name and Resident Registration Number written in Resident Register
  - ② Name and Registration Number written in Registered Foreigners Record according to the Immigration Control Act
- Corporation
  - ① Name of Corporation and Business Registration Number stated in Business Registration Certificate
  - ② Corporation's Name and Tax Payment No. as stated in the document provided according to the Corporate Tax Act if a corporation does not received a business registration certificate
- Organization other than Corporation
  - ① The Name and resident registration number of the organization's representative as stated in the resident register (Or name and registration number as stated in foreigner registration records if the representative is a foreigner)
  - ② Organization's name and Reference No. or Tax Payment No. as stated in the document if the organization is granted Reference No. according to the Value Added Tax Act or Tax Payment No. under the Income Tax Act
- Other Real Name Verification as Prescribed by Minister of Pubic Administration and Security

It shall be ascertained the authenticity of the identity between the applicant and the named person by the following proof for verifying identity.

- Individual
  - ① Resident Registration Card if s/he is an eligible person to being issued the card. Provided if it is difficult to use a resident registration card, a copy of proof issued by the national or a local government authority and/or school principal according to the primary/ middle school education laws that may verify the identity
  - ② A copy of proof issued by the national or a local government authority and/or school principal according to the primary/middle school education laws that may verify the

identity or the applicant's residence register and his/her legal representative's proof as stated in ① of this section if the applicant is not the eligible to being issued the Resident Registration Card

③ Passport or Overseas Residents Registration Card if s/he is an overseas resident

④ Foreigner Registration Card according to the Immigration Control Act if if s/he is a foreigner. Provided if the Foreigner Registration Card is not issued, Passport or Identification Card

- Corporation
  ① Company Register or Commerce Register, Business Registration Certificate, Document or its Copy that showing the grant of Tax Payment No.
- Organization other than Corporation
  ① Identification proof according to Article 13.3 of the Enforcement Rule of the Act, including the proof as stated in ① of "Individual" case which allows to verify the identity of the organization's representative.
- Other Proof for Identity Verification as Prescribed by Minister of Pubic Administration and Security

3.2 New Issuance of Certificates

3.2.1 Methods for Identity Verification

CrossCert verifies the identity considering the scope of use for authorized certificates as prescribed in Article 15 (Issuance of Authorized Certificate), Article 18-2 (Personal Identification by Authorized Certificate) of the Act and Article 4 (Methods for Identity Verification) of Guide on Identity Verification Works of Licensed Certification Authorities etc. and the principles are as the followings.

- It is the principle to verify the identity by face to face meeting in the case of the new subscriber. Provided the identity verification may be regarded as performed if the applicant has been verified its identity through the face to face meeting in the reliable organizations including financial institutes or public authorities etc.
- Identification verification may be performed by a valid authorized certificate issued by CrossCert or other licensed certification authorities.
- Identity verification for a subscription applicant of specific authorized certificates may be performed by adopting quasi-meeting methods.
- Authorized certificate shall be issued only to the subscriber who completed the identity verification procedure.

- When the document submitted, it is sufficient to provide only the changed items compare to that of the initial application. In this case, the major online contact details of the subscription applicant shall be included.

3.2.1.1 Identity Verification on Individuals

When the identity verification on the individuals are performed, the verification shall be made by ascertaining photograph etc on the identification certificate etc as well as name and resident registration number on the relevant documents provided according to 3.1.1 of this Certification Practice Statement. Provided other identification certificates may be alternatively used if it is impracticable to verify the identity from the photograph of the identification certificate provided from the applicant.

3.2.1.2 Identity Verification on Corporations

When the identity verification on the corporations are performed, the verification shall be made by ascertaining its name, address of office, representative's name, business registration number etc as stated in the submitted documents according to 3.1.2 of this Certification Practice Statement and the verification for the representative's identity of the corporation or organization shall be performed. Provided, the agent's identity shall be verified upon the receipt of power of attorney granted from the representative, if the agent made an application.

3.2.1.3 Identity Verification on a Subscriber Who Has Already Issued

If an existing subscriber of CrossCert applies the reissuance, renewal, suspension and revocation of the authorized certificate through providing the digital signature on its application form by using his/her valid digital signature creating key, the subscriber's identity may be verified by the digital signature and the authorized certificate. The verification of the identity shall be performed by verifying the registered information and the digital signature by the digital signature verifying key. Provided, however the applied facts shall not be acknowledged, if the subscriber's authorized certificate is in the suspension status.

3.2.2 Transmission Methods for Subscriber Information and Security Methods for Confidentiality, Integrity etc. of Subscriber Information

Afterr the identity verification is completed, subscription applicant or its agent visits CrossCert's web-site and downloads "Subscriber Authorized Certificate Management Program", then creates a digital signature key and requests for issuance of an authorized certificate by inputting Reference

No./Approval Code. A certain part of the foregoing issuance request process may be automatically processed by the subscriber's software.
CrossCert guarantees the confidentiality and integrity etc of the subscriber's information by the application of the encryption according to the encryption algorithm as stated in Article 5.1.3 of Rules on the Facilities and Equipments etc of Licensed Certification Authority and Registration Authority's authorized digital signature in relation to the subscriber's registered information, if it receives the registered information of the applicant for an authorized certificate through the information telecommunication networks from a registration authority.

CrossCert guarantees the confidentiality and integrity etc of the subscriber's information by the application of the encryption according to the encryption algorithm as stated in Article 5.1.3 of Rules on the Facilities and Equipments etc of Licensed Certification Authority and Registration Authority's authorized digital signature in relation to the subscriber's registered information, if it transmits the subscriber's registered information through a transmission service provider between a registration authority and CrossCert.

CrossCert issues an authorized certificate after ascertaining the following matters when it provides a new issuance of the authorized certificate.

- Identity verification according to the verification procedure for the new issuance of authorized certificate as stated in this Certification Practice Statement
- Verifying the uniqueness of the digital signature verifying key submitted by the subscription applicant of an authorized certificate
- Verifying whether it holds the matching digital signature creating key to the digital signature verifying key submitted by the subscription applicant of an authorized certificate
- Verifying the uniqueness of the subscriber's Distinguished Name submitted by the subscription applicant of an authorized certificate
- Verifying the consentaneity between the subscriber's Distinguished Name and Identification submitted by the subscription applicant of an authorized certificate

The newly issued authorized certificate is registered in the directory of CrossCert at the same time when it is issued.

3.2.3 Proving Methods for Owning Digital Signature Creating Key by Subscriber

Subscriber submits the information that has its digital signature by his/her digital signature creating key to CrossCert, and then CrossCert issues an authorized certificate after verifying the fact that the subscriber owns the digital signature creating key by ascertaining whether the

subscriber's digital signature creating key and digital signature verifying key are matched each other through the process of the verification on the submitted information by the digital signature verifying key.

3.2.4 Expression Methods and Guaranteeing Uniqueness of Distinguished Name of Subscriber

Names used in the basic field of an authorized certificate, its suspension and revocation list shall be applied with the Distinguished Name methods according to X.500.

① Expression of Distinguished Name
CrossCert accommodates the following items in relation to the name of the subscriber in the issuance of an authorized certificate.

- Legal Name, including Real Name of Individual, Name of Corporation, etc(English Name)
- Internet Domain Name
- Internet IP Address
- Internationally known or recognized by Korean Intellectual Property Office Trademark etc. with the accompanying relevant certificates
- URL for WWW
- Electronic Mail Address etc.

Provided, it may be allowed to be written through a separate negotiation if the subscriber requests for a different name.

② Guaranty Methods of the Uniqueness of Distinguished Name
Distinguished Name shall be stored with the composition of the submitted information according to the prescribed standard. At the time, an authorized certificate is issued only when it is not overlapped in the duplicity test procedure because Distinguished Name becomes the standard information that may be used for a user to verify the authorized certificate. If Distinguished Name is overlapped, the subscriber may be requested to provide new Distinguished Name and the subscriber must follow on the request if he/she desires to use the certification service.

3.2.5 The Way Subscriber Receives Authorized Certificate

CrossCert provides an authorized certificate issuance code to the applicant after it verified the identity of the applicant and the authenticity of the application documents according to this Certification Practice Statement, then the applicant accesses to the certification system of CrossCert and agree to the Certification Service Agreement and input the received issuance code,

subsequently to the foregoing the applicant receives an authorized certificate by downloading.

3.3 Renewal of Authorized Certificates

3.3.1 Requirements for Renewal Issuance, Applicants and Application Process

① Requirements

If a subscriber requests the extension of the validity period without changing the existing digital signature creating key that the subscriber has used AND if it is before the expiry date of an authorized certificate, the validity period for the authorized certificate may be extended for the same period to that of the initial subscription according to 3.1 (Application for Issuance of Authorized Certificate) and 2.1 (Types of Authorized Certificates). (However, the validity period may be limited by the discretion of CrossCert at the time.)

Consecutive renewal without the change of the subscriber's digital signature creating key more than once cannot be allowed because it may cause a security problem.

② Applicant and Application Procedure

The application may be made only by the renewal screen of CrossCert without via a registration authority and the identity verification shall be regarded as completed by the subscriber's digital signature because the availability of a renewal should be processed in consideration of the security matters and other circumstances.

CrossCert issues an authorized certificate having the new validity period after reviewing the renewability of the authorized certificate.

In the event that an authorized certificate renewed, the subscriber's information included in the authorized certificate shall not be changed and only the validity period for the authorized certificate shall be changed. If a subscriber intends to change any contents of the authorized certificate, she/he should receive the newly issued authorized certificate by applying for the re-issuance of an authorized certificate.

3.3.2 Transmission Methods for Subscriber Information and Security Methods for Confidentiality, Integrity etc. of Subscriber Information

It applies 3.2.2 of this Certification Practice Statement correspondingly.

3.3.3 Proving Methods for Owning Digital Signature Creating Key by Subscriber

It applies 3.2.3 of this Certification Practice Statement correspondingly.

3.3.4 Expression Methods and Guaranteeing Uniqueness of Distinguished Name of Subscriber

It applies 3.2.4 of this Certification Practice Statement correspondingly.

3.3.5 The Way Subscriber Receives Renewed Authorized Certificate

CrossCert issues the renewed authorized certificate after reviewing the renewability of the authorized certificate and the subscriber receives the authorized certificate with having the new validity period if a subscriber applies for the renewal of an authorized certificate via the online. The identity verification in this case may be replaced by the subscriber's digital signature.

3.4 Reissuance of Authorized Certificates

3.4.1 Requirements for Re-Issuance, Applicants and Application Process

① Requirements and Applicants
Subscriber may revoke the existing authorized certificate and apply for the new authorized certificate if it is necessary due to the existing authorized certificate's security, change of business registration number or business name, change of status from self-employed to corporation, or change of the information included in the authorized certificate such as transferring issuance from specific purpose to general use etc.

② Application Procedure
Once a subscriber submits the re-issuance application form according to the relevant procedure by visiting a registration authority or CrossCert, a registration authority or CrossCert applies for the re-issuance of the authorized certificate.

If an authorized certificate is re-issued, the existing authorized certificate shall be automatically revoked and the validity period for the re-issued authorized certificate shall be the remaining period after deducting the used period out of one year which was set at the time of the initial issuance of the previously existed authorized certificate and therefore the expiry date shall not be changed. At the time the authorized certificate shall be created and issued to the subscriber by using the new digital signature verifying key and the existing Distinguished Name.

3.4.2 Identity Verification Method on Re-Issuance Applicant

If an existing subscriber of CrossCert applies the reissuance of the authorized certificate through providing the digital signature on its application form by using his/her valid digital signature creating key, the subscriber's identity may be verified by the digital signature and the authorized certificate. The verification of the identity shall be performed by verifying the registered information and the digital signature by the digital signature verifying key. Provided, however the applied facts shall not be acknowledged, if the subscriber's authorized certificate is in the suspension status.

3.4.3 Transmission Methods for Subscriber Information and Security Methods for Confidentiality, Integrity etc. of Subscriber Information

It applies 3.2.2 of this Certification Practice Statement correspondingly.

3.4.4 Proving Methods for Owning Digital Signature Creating Key by Subscriber

It applies 3.2.3 of this Certification Practice Statement correspondingly

3.4.5 Expression Methods and Guaranteeing Uniqueness of Distinguished Name of Subscriber

It applies 3.2.4 of this Certification Practice Statement correspondingly.

3.4.6 The Way Subscriber Receives Re-Issued Authorized Certificate

It applies 3.2.5 of this Certification Practice Statement correspondingly.

3.5 Change of Subscriber's Registered Information

3.5.1 Identity Verification on Change Requirements, Applicant, Application Procedure and Applicant who filing the Change

CrossCert verifies the identity by adopting various verification methods according to the reasons for the issuance with changing information thereof if a subscriber applies due to the existing authorized certificate's security, change of business registration number or business name etc. Provided that the identity verification may be performed according to the prescribed procedure as in 3.2.1.3 (Identity Verification on a Subscriber Who Has Already Issued) of this Certification

Practice Statement if the subscriber holds a valid digital signature creating key.

① When the issuance with changing information is applied due to the security problems

- Applicable Objects: Damaged Authorized Certificate, Lost Password for Digital Signature
- Documents for Submission
  - Application Form of Authorized Certificate
    - Specify the Approval Code received at the time of new issuance made in the Application Form
- Identity Verification Methods:
  - Ascertaining the authenticity by comparing documents submitted at the time of the initial issuance with the documents additionally submitted
    - Checking the sameness of the information written in the application documents, seal impression, and approval code
  - Device issued after the identity verification is made (OTP, Table of Random Card etc)
  - Verifying the identity by confirming through customer center of CrossCert
    - Personal Information including Name (Corporation's Name), Resident Registration No.(Business Registration No.) etc.
    - Contact Information including Telephone No., Address, and Electronic Mail etc.
    - "Question" and "Answer" that the subscriber initially stated and prepared when he/she made the new issuance application for verifying in case of the urgent revocation/suspension

② When the issuance with changing information is applied due to the change of authorized certificate's information

- Applicable Objects: Change of Business Name or Business Registration No., Transferring Issuance from Specific Purpose to General Use of Authorized Certificates
- Documents for Submission
  - Documents as stated in 3.1.1 (Filing Application for Authorized Certificate Issuance)
- Identity Verification Methods: Corresponding procedure to 3.2 (New Issuance of Certificates)

3.5.2 Transmission Methods for Subscriber Information and Security Methods for Confidentiality, Integrity etc. of Subscriber Information

It applies 3.2.2 of this Certification Practice Statement correspondingly.

3.5.3 Proving Methods for Owning Digital Signature Creating Key by Subscriber

It applies 3.2.3 of this Certification Practice Statement correspondingly.

3.5.4 Expression Methods and Guaranteeing Uniqueness of Distinguished Name of Subscriber

It applies 3.2.4 of this Certification Practice Statement correspondingly.

3.5.5 How to Receive Authorized Certificate that Has Been Changed Its Registered Information

It applies 3.2.5 of this Certification Practice Statement correspondingly.

3.6 Suspension, Recovery, and Revocation of Authorized Certificates

3.6.1 Application Requirements, Applicant and Application Procedure

3.6.1.1 Suspension Requirements for Authorized Certificate's Validity

- CrossCert suspends the validity of an authorized certificate by the application of the subscriber or its agent if the subscriber desires to suspend the validity of the authorized certificate.
- CrossCert has the right to suspend the validity of the authorized certificate if the Minister of Public Administration and Security orders according to Article 16.2 of the Act or it occurred the inevitable reasons in relation to operation of the certification service although the subscriber does not apply.

3.6.1.2 Applicant and Application Procedure for Authorized Certificate's Validity Suspension

The subscriber who intends to apply for the validity suspension shall access to the suspension screen of CrossCert's web-site and make the application through online OR he/she may apply for the validity suspension by visiting a registration authority in person. The identity verification may be replaced by the subscriber's digital signature if a subscriber applies for the validity suspension through online.

In case the system is not accessible or she/he is unable to visit a registration authority, she/he may apply for the validity suspension by calling CrossCert's customer support team (Tel: 1566-0566). CrossCert receives the application for the validity suspension of an authorized certificate after performing the identity verification.

Provided, the subscriber shall formally undertake the validity suspension by visiting a registration authority or CrossCert in person within 7 days from the application if he/she made the application for the validity suspension through the telephone line. Otherwise, the validity suspension will be cancelled and it will be available to use at normal functions.

3.6.1.3 Applicant and Application Procedure for Authorized Certificate's Validity Recovery

The validity of the authorized certificate shall be recovered if the subscriber applies for the validity recovery within 6 months from the commencement date of the validity suspension OR if the temporarily suspended authorized certificate due to the order of the Minister of Public Administration and Security according to Article 16.2 of the Act needs to be recovered its validity. In this case, the validity period of the recovered authorized certificate is not changed.

Validity recovery may not be processed through the online because the suspended authorized certificate is under the status of suspension unlike the time of the suspension application made, therefore the applicant must visit a registration authority or CrossCert in person for making the validity recovery application. In addition, the validity recovery may not be applied through the telephone line.

Once a subscriber submits the validity recovery application form according to the relevant procedure by visiting a registration authority or CrossCert, a registration authority or CrossCert applies for the validity recovery of the authorized certificate to CrossCert after they perform the identity verification procedure.

CrossCert processes the applied matters in a prompt manner and deletes the relevant authorized certificate from the validity suspension list if it receives a validity recovery application from a registration authority or CrossCert's customer support team.

3.6.1.4 Revocation Requirements for Authorized Certificate

A subscriber has a right to revoke the authorized certificate according to Article 18 (Revocation of Authorized Certificate) of the Act and the revoked authorized certificate cannot be recovered its validity. CrossCert may revoke the relevant authorized certificate if one of the following events occurs.

- If a subscriber or its agent desires to revoke the authorized certificate
- It is acknowledged the facts that a subscriber received the authorized certificate by the

fraudulent conduct or other unlawful ways

- It is acknowledged the facts that a subscriber is dead, adjudicated as disappearance, or dissolved
- If no validity recovery application has been made for the authorized certificate suspended according to 3.6.1 of this Certification Practice Statement within 6 months from the commencement date of the validity suspension
- If CrossCert's digital signature creating information is leaked

3.6.1.5 Revocation Procedure for Authorized Certificate

The subscriber who intends to apply for the revocation shall access to the revocation screen of CrossCert's web-site and make the application through online OR he/she may apply for the revocation by visiting a registration authority or CrossCert in person. The identity verification may be replaced by the subscriber's digital signature if a subscriber applies for the revocation through online. The revocation of the authorized certificate may not be applied through the telephone line. Provided, it can only apply for the validity suspension first through the telephone line and prevent from being used.

3.6.2 Identity Verification on the Applicant

CrossCert verifies the applicant's identity according to the corresponding procedures to the new issuance application if a subscriber applies for the validity suspension and revocation of the authorized certificate. Provided that the identity verification may be performed according to the prescribed procedure as in 3.2.1.3 (Identity Verification on a Subscriber Who Has Already Issued) of this Certification Practice Statement if the subscriber holds a valid digital signature creating key. Further, the identity verification may be replaced by confirming "Question" and "Answer" that the subscriber initially stated and prepared when he/she made the new issuance application for verifying in case of the urgent revocation/suspension through the telephone line.

CrossCert verifies the applicant's identity according to the corresponding procedures to the new issuance application if a subscriber applies for the validity recovery of the authorized certificate.

3.6.3 Issuing Period and Public Notification of Authorized Certificate Suspension and Revocation List (CRL)

CrossCert shall make a notification promptly upon the occurrence of the changes in relation to the licensed certification services, including the validity suspension of the authorized certificate, revocation list of the authorized certificate. The validity suspension of authorized certificates and

revocation list of authorized certificates shall be updated regularly by once a day, maximum 24 hour basis and it shall be publicly notified that anyone may check the facts by the certification management system.

3.6.4 Capable Period to Maintain the Suspension Status of Authorized Certificate

Once validity suspended authorized certificate may only be retained for 6 months from the validity suspension according to Article 17 (Suspension etc. of Validity of Authorized Certificate) of the Act and the validity suspended authorized certificate shall be automatically revoked if no application is made for the validity recovery within the said 6 months period. Provided, if the expiry date comes within the suspension period, it shall be regarded as the same case to the expiry of an authorized certificate.

3.7 Online Certificates Status Protocol Service of Authorized Certificate

3.7.1 Online Certificates Status Protocol Service of Authorized Certificate

Online Certificates Status Protocol Service of Authorized Certificate provided by CrossCert means the service enabling a user to ascertain the revocation and suspension status of authorized certificates in real-time.

The applicant or its agent should submit the application form of Online Certificates Status Protocol Service to a registration authority or CrossCert.

A subscriber of CrossCert's Online Certificates Status Protocol Service requests for the validity confirmation of his/her authorized certificate through the software of Online Certificates Status Protocol Service received from a registration authority or CrossCert.

CrossCert provides the status information to a user upon the user's request for the status of an authorized certificate.

3.7.2 Termination of Agreement on Online Certificates Status Protocol Service of Authorized Certificate

If the subscriber intends to terminate Online Certificates Status Protocol Service, he/she applies for the termination upon submitting the termination application form to CrossCert. Upon the receipt of the termination application form, CrossCert promptly terminates the relevant service

agreement and notifies the termination to the applicant. Provided, the termination of Online Certificates Status Protocol Service shall not prejudice to each party's rights resulted prior to the termination.

3.8 Miscellaneous Additional Services

3.8.1 Time-Stamping Service

Time-stamping token provided to the user of the time-stamping service from CrossCert is being used to prove that a certain data in question existed at the specific time.

The applicant or its agent should submit the application form of the time-stamping service to a registration authority or CrossCert. After the registration procedure, a registration authority or CrossCert provides a confirmation of registration for the time-stamping service including the account for the service to the applicant or its agent.

The subscriber of the time-stamping service of CrossCert requests a time-stamping token in relation to the relevant data after being confirmed its own time-stamping account by using the time-stamping software provided by a registration authority or CrossCert or the subscriber's own software.

Upon the receipt of the request for the time-stamping token, CrossCert verifies the requesting person and ascertains the effectiveness of the requested information, and then issues the time-stamping token for the requested data. CrossCert replies an error message stating that the service is unavailable if it cannot provide the reply on the time-stamping request within one minute.

CrossCert provides the requesting person the replying information on the time-stamping request including the following items.

- Name of Time-Stamping Organization
- Serial No. of Time-Stamping Token
- Policy of Time-Stamping Organization
- Issuance Time of Time-Stamping Token
- Hash Value
- Hash Algorithm
- Information on Authorized Certificate of Time-Stamping Organization
- Signature of Time-Stamping Organization

- Other Necessary Information for Time-Stamping Service

The subscriber of the time-stamping service shall submit the information including the following items through the information telecommunication networks when she/he requests for the time-stamping token.

- Hash Value
- Hash Algorithm
- Other Necessary Information for Time-Stamping Service

3.8.2 Termination of Agreement on Time-Stamping Service

If the subscriber intends to terminate Time Stamping Service, he/she applies for the termination upon submitting the termination application form to CrossCert. Upon the receipt of the termination application form, CrossCert promptly terminates the relevant service agreement and notifies the termination to the applicant. Provided, the termination of Time Stamping Service shall not prejudice to each party's rights resulted prior to the termination.

3.9 Profile of Authorized Certificate

3.9.1 Composition and Contents of Authorized Certificate

CrossCert complies with the technical standard for the digital signature certification as prescribed in the [Rules on the Facilities and Equipments etc of Licensed Certification Authority] published by Ministry of Public Administration and Security and it issues the authorized certificate conforming X.509 V3 Standards.

CrossCert complies with the [Technical Standards for Digital Signature Authorized Certificate Profile] as prescribed by Korea Internet & Security Agency, and the Profile of Authorized Certificates are as the followings.

1) Basic Field

#	Field Name	ASN.1 type	Note	Support		Remarks
				Creation	Processing	
1	Version	INTEGER	0x2(version 3)	m	m	

2	Serial Number	INTEGER	Automatic allocation	m	m	
3	Issuer type value	 OID printableString or utf8String	[KCAC.TS.DN] Compliance C(Country) is printableString,, the property figures for others are utf8String	m m m	m m m	
4	Validity notBefore notAfter	 UTCTime UTCTime	Compliance with the validity period as stated in the highest certification authority's CPS	m m m	m m m	
5	Subject type value	 OID printableString or utf8String	[KCAC.TS.DN] Compliance C(Country) is printableString,, the property figures for others are utf8String	m m m	m m m	
6	Subject Public Key Info algorithm subjectPublicKey	 OID BIT STRING		m m m	m m m	
7	Extensions	Extensions		m	m	

2) Extension Field

#	Field Name	ASN.1 type	Note	C	Support		Remarks
					Creati	Proce	
1	Authority Key Identifier KeyIdentifier authorityCertIssuer authorityCertSerialNumber	 OCTET STRING GeneralNames INTEGER	Issuer's Certificate KeyID	n	m m m m	m m m m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 160bits Hash Value of Info.	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	Certificate Policy policyIdentifier policyQualifiers PolicyQualifierId Qualifier CPSuri	 OID OID IA5String	 CPS policy of licensed certification authority CPS, UserNotice licensed certification authority	b	 m m m m m	 m m m m m	[1]

	UserNotice NoticeReference ExplicitText	 SEQUENCE BMPString	CPS address		m - m	m - m	
5	Policy Mappings issuerDomainPolicy subjectDomainPolicy	 OID OID		-	-	-	
6	Subject Alternative Names	otherName	id-kisa-identifyData Subscriber Real Name VID	n	m	m	
		rfc822Name	Subscriber Email Address		o	m	[2]
7	Issuer Alternative Names	otherName	id-kisa-identifyData licensed certification authority Korean real Name	n	o	m	
8	Extended Key Usage	OID	Security Token(id-kisa-HSM)	n	o	o	[3]
9	Basic Constraints cA pathLenConstraint	 FALSE INTEGER		-	x	x	
10	Policy Constraints requireExplicitPolicy inhibitPolicyMapping	 INTEGER INTEGER		-	-	-	
11	Name Constraints			-	-	-	
12	CRL Distribution Point distributionPoint reasons cRLIssuer	 DistributionPointName ReasonFlags GeneralNames	 CRL Acquired Info. Used Indirect CRL Issuance	n	m m - o	m m - m	[4]
13	Authority Information Access accessMethod accessLocation	 OID GeneralName	id-ad-caIssuers, id-ad-ocsp	n	m m m	m m m	[5]
[1]	Set-Up hon-critical' for the Use of Email Security, Otherwise, recommend to set-up 'critical'						
[2]	Recommend the Creation of rfc822Name for the Use of Email Security						
[3]	Use the Security Token (id-kisa-HSM) for the security basis of [KCAC.TS.HSM]						
[4]	Use uri ldap://hostname[:portnumber]/dn[?attribute] Type						
[5]	Recommend the Creation of id-ad-caIssuers for the Use of Email Security						

Items included in an authorized certificate are containing the following contents in addition to the items according to Article 15.2 of the Act.

- Subscriber's Name
- Subscriber's Digital Signature Verifying Key
- Digital Signature Methods used by Subscriber and Licensed Certification Authority
- Serial No. of Authorized Certificate
- Validity Period of Authorized Certificate
- Name of Licensed Certification Authority

- Relevant Information of Authorized Certificate If the Scope of Use or Purpose of Use is Limited
- Relevant Information If Subscriber Has an Agent's Authority for a Third Party
- Indication of Licensed Certification Authority

3.10 Profile of Authorized Certificate's Suspension and Revocation List

3.10.1 Composition and Contents of Authorized Certificate's Suspension and Revocation List

CrossCert complies with the technical standard for the digital signature certification as prescribed in the [Rules on the Facilities and Equipments etc of Licensed Certification Authority] published by Ministry of Public Administration and Security and it issues the suspension and revocation list of authorized certificates conforming X.509 V3 Standards.

CrossCert identifies that the validity of the authorized certificate has been suspended by using the revocation reasons field out of the extension field in the suspension and revocation list if it suspends the authorized certificate.

CrossCert complies with the [Technical Standards for Digital Signature Authorized Certificate's Suspension and Revocation List Profile] as prescribed by Korea Internet & Security Agency, and the Profile of Authorized Certificate's Suspension and Revocation List is as the followings.

1) Basic Field

#	Field Name	ASN.1 type	Note	Support		Remarks
				Creati	Proces	
1	Version	INTEGER	0x1(Version 2)	m	m	
2	Signature	OID	Automatically allocated	m	m	
3	Issuer		[KCAC.TS.DN] Compliance	m	m	
	type	OID	C(Country) is printableString,, the property	m	m	
		printableString	figures for others are utf8String			
	value	또는 utf8String		m	m	
4	This Update	UTCTime	Upon Issuance	m	m	
5	Next Update	UTCTime	Complying Policy of Licensed CA	m	m	

6	Revoked Certificates userCertificate revocationDate crlEntryExtensions	INTEGER UTCTime Extensions		 m m	 m m	[1] [2]
7	CRL Extensions	Extensions		m	m	[3]
[1]	Revoked Certificates Field does not created if no suspended or revoked certificate exists					
[2]	Refer to the below "3) CRL Entry Extension Field"					
[3]	Refer to the below "2) CRL Entry Extension Field"					

2) CRL Extension Field

#	Field Name	ASN.1 type	Note	C	Support		remarks
					creation	processi	
1	Authority Key Identifier KeyIdentifier authorityCertIssuer authorityCertSerialNumber	OCTET STRING GeneralNames INTEGER	KeyID of Certification Authority	n	m	m	
2	Issuer Alternative Name	otherName	id-kisa-identifyData Certification Authority	n	o	m	
3	CRL Number	INTEGER		n	m	m	
4	Issuing Distribution Point DistributionPointName onlyContainsUserCerts onlyContainsCACerts onlySomeReasons IndirectCRL	IA5string BOOLEAN BOOLEAN BIT STRING BOOLEAN		c	m m - - - o	m m - - - m	 [1]
[1]	Same to CRLDP(Certificate Revocation List Distribution Point) ※ Refer to [KCAC.TS.DSCP]						
[2]	Set-up "TRUE" When using indirectCRL						

3) CRL Entry Extension Field

#	Field Name	ASN.1 type	Note	C	Support		remarks
					creation	processi g	
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	

3.11 Profile of Authorized Certificate's Online Certificates Status Protocol Service (OCSP)

3.11.1 Composition and Contents of Authorized Certificate's Online Certificates Status Protocol Service (OCSP)

CrossCert complies with the [Technical Standards for Status Verification for Authorized Certificates in Real Time] as prescribed by Korea Internet & Security Agency in order to provide Authorized Certificate's Online Certificates Status Protocol Service in real time for preserving the credibility of the use of certification services under the certification system, and the Profile of Authorized Certificate's Online Certificates Status Protocol Service is as the followings.

1) Basic Field

#	Field Name	ASN.1 type	Note	Support		Remarks
				creat	Proce	
1	Version	INTEGER	0x2(Version 3)	m	m	
2	Serial Number	INTEGER	Automatically allocated	m	m	
3	Issuer type value	 OID printableString or utf8String	[KCAC.TS.DN] Compliance C(Country) is printableString,, the property figures for others are utf8String	m m m	m m m	
4	Validity notBefore notAfter	UTCTime UTCTime	Compliance Expiry as stated in the Highest CA's CPS	m m m	m m m	
5	Subject type value	OID printableString or utf8String	[KCAC.TS.DN] Compliance C(Country) is printableString,, the property figures for others are utf8String	m m m	m m m	
6	Subject Public Key Info algorithm subjectPublicKey	OID BIT STRING		m m m	m m m	
7	Extensions	Extensions		m	m	

2) Extension Field

#	Field	ASN.1 type	Note	C	Support		Remarks
					creati	Proce	
1	Authority Key Identifier KeyIdentifier authorityCertIssuer authorityCertSerialNumber	OCTET STRING GeneralNames INTEGER	Using all of 3 values	n	m m m m	m m m m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey info. 160bits Hash Value	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	

4	Certificate Policy policyIdentifier policyQualifiers PolicyQualifierId Qualifier CPSuri UserNotice NoticeReference ExplicitText	 OID OID IA5String SEQUENCE BMPString	 Policy of Licensed CA CPS, UserNotice CA CPS Address Compliance with Certificate Expression Standard	c	 m m m m m m - m	 m m m m m m - m	
5	Policy Mappings			-	-	-	
6	Subject Alternative Names	otherName	id-kisa-identifyData 0| Subscriber KoreanName	n	m	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData 0| Issuing Authority KoreanName	n	o	m	
8	Basic Constraints			-	x	x	
9	Policy Constraints			-	-	-	
10	Name Constraints			-	-	-	
11	Extended Key Usage	OID		c	m	m	
12	CRL Distribution Point distributionPoint reasons cRLIssuer	DistributionPointName ReasonFlags GeneralNames	CRL Acquired Info. Used When Indirect CRL Issuance	n	m m o o	m m m m	[1]
13	Authority Information Access accessMethod accessLocation	OID GeneralName	id-ad-caIssuers	n	o	m	[2]
14	OCSP No Check	OID	id-pkix-ocsp-nocheck	n	o	m	[3]
[1]	Use ldap://hostname[:portnumber]/dn[?attribute] as Uri Value						
[2]	When Certification Authority Issues OCSP Server Certificates, Must Create. Not be Used for Time-Stamping Certificates						
[3]	Used if OCSP Server shortlived Certificates is ibeing ssued Not be Used for Time-Stamping Certificates						

3.12 Renewal of Digital Signature Key by CrossCert

CrossCert applies for the re-issuance of the authorized certificates to Korea Internet & Security Agency by creating the new digital signature key prior to the expiry date of the authorized certificates. CrossCert notifies the subscriber and the user upon the issuance of the new authorized certificates of CrossCert and takes proper measures thereon.

Subscriber shall apply for the re-issuance of the authorized certificates to Korea Internet & Security Agency by creating the new digital signature key prior to the expiry date of its authorized certificates.

3.13 Suspension and Revocation of Licensed Certification Work

When CrossCert desires to cease or close all or part of its licensed certification service due to its circumstances, it shall fix the cessation period and the scheduled cessation date and the scheduled closure date, furthermore it shall report to its subscribers and the Minister of Public Administration and Security by submitting "Certification Work (Cessation/Closure) Report" not later than 30 days before the scheduled cessation date in case of cessation, not later than 60 days before the scheduled closure date in case of closure, according to Article 7 of the Enforcement Rules of the Act.

CrossCert's cessation period of certification work onto subscribers shall not exceed 6 months and CrossCert shall transfer its subscribers' authorized certificates and the records regarding validity suspension and revocation to another licensed certification authority if it reported the closure of certification work.

3.14 Discontinuance of Licensed Certification Work or Cancellation of Designating the Licensed Certificate Authority

CrossCert may receive the suspension order for its certification work or the designation as a licensed certification authority may be revoked by Article 12 (Suspension of Certification Work or Revocation of Designation, etc.) of the Act. Main reasons are as the followings.

- Where a designation as provided in Article 4 of the Act was obtained through fraud or any other wrongful means
- Where a licensed certification authority which has been ordered to suspend its certification work fails to suspend the certification work in violation of such order
- Where certification work is not commenced within 6 months after designation as provided in Article 4 of the Act or where certification work is ceased for more than 6 or more consecutive months
- Where an order to amend Certification Practice Statement according to Article 6.4 of the Act is violated

CrossCert shall transfer its certification work to another licensed certification authority in a prompt manner when its designation as a licensed certification authority has been revoked. Provided, when it is impossible for CrossCert to transfer its work due to the circumstances of the purported licensed certification authority, CrossCert shall report it to the Minister of Public Administration and Security by submitting 'Letter of Reasons for Impossibility of Transferring Subscriber's

Authorized certificates etc.' and 'Lists for Transferring Subscriber's Authorized certificates etc.'

Chapter 4. Public Notification of Information Relevant to Licensed Certification Work

4.1 Facility for Public Notification

CrossCert shall operate the notification facility for notifying the information in relation to the issuance and management of authorized certificates including Certification Practice Statement, authorized certificates, authorized certificate's validity suspension and revocation lists etc (hereinafter, "Information Regarding Certification Work") that allows anybody may confirm its contents and it shall publicly notify the change of Information Regarding Certification Work whenever it is changed without delay.

4.2 Methods for Public Notification

CrossCert shall make a public notification for Information Regarding Certification Work through the information storage location in the facility as stated in 4.1 of this Certification Practice Statement. It owes a responsibility to make a notification immediately upon the completion of the relevant work according to 3.6.3 (Issuing Period and Public Notification of Authorized Certificate Suspension and Revocation List (CRL)) of this Certification Practice Statement when the contents of Information Regarding Certification Work are changed.
CrossCert's storage and notification sites for Information Regarding Certification Work are as the followings.

Information related to CrossCert

Certification Practice Statement	http://gca.crosscert.com/cps.html
Authorized Certificate	http://gca.crosscert.com/cacert.html
Authorized Certificate's Validity Suspension and Revocation List	ldap://dir.crosscert.com
Information on Registration Authority	http://gca.crosscert.com/partner/pa_registration.html

Information related to Korea Internet & Security Agency

Certification Practice Statement	http://www.rootca.or.kr/rca/cps.htm
List of Licensed Certification Authority	http://www.rootca.or.kr/lca/lca.htm
List of Authorized Certificates	http://www.rootca.or.kr/cert.htm
Authorized Certificate's Validity Suspension and Revocation List	http://www.rootca.or.kr/crl.htm

Chapter 5. Protective Measures on Facilities and Equipments Relevant to Licensed Certification Work

5.1 Physical Protective Measures

5.1.1 Separation of Licensed Certification System Operating Room

CrossCert shall install and operate the core certification system in the separate restricted area by each core certification system in order to protect the core certification systems.

CrossCert install and operate the core certification system in the security cabinet in order to protect the system and restrict the physical access thereto.

5.1.2 Controlling Physical Access

CrossCert controls the physical access in order to protect the site where the core certification system etc is installed from the physical threats including an invasion, unlawful access trial etc as the followings.

- Only an authorized person is allowed to access to the certification center of CrossCert.
- CrossCert's access control system restricts the access to the core certification system and restrictive area in multiple combinations of access restriction devices based on location/knowledge/biometrics.
- CrossCert controls physical access of a visitor except for the special circumstance (repairing hardware etc.) and the responsible personnel shall accompany the visitor when it is necessary for the visitor's access.
- CrossCert controls access 24 hours a day and records all persons entering the certification center and periodically stores the entry record to the back-up facility and preserves in the safe location.
- CrossCert installs and operates the security monitor equipments for 24 hour surveillance and monitoring control system with alarming functions.
  - CCTV Camera Installing in exits and all of the major places in the certification center
  - To install and operate surveillance system which is able to monitor 24 hours a day
  - Installing the monitoring equipments for detecting the invasion covering all the area of certification center

- CrossCert operates the 24 hour security system under the contract with a licensed security company.

5.1.3 Prevention of Fire, Water Exposure, Power Failure and Protection etc.

CrossCert established the core certification system and major facilities in the place higher than 30 cm from the surface to prevent the water exposure in the case and operates ventilation/temperature and humidity controller for preventing from damages due to the humidity.

CrossCert installs fire alarming equipments in the core certification system room and certification center and portable fire extinguishers and automatic fire extinguishing facilities in the core certification system room etc. In addition, it prepares the fire extinguishing devices not adversely affect the systems when it is used.

CrossCert uses the 'non black-out' power supply equipment and self-generating power facilities which are capable to ensure the continuous certification work upon the occurrence of power failure. When the prepared back-up power exhausted the 'non black-out' power equipment shuts down the system power in the safe manner to minimize the loss of the system.

5.1.4 Equipment and Facility Disposal Procedure

CrossCert physically destroys to make it impossible to recovery under the attendance of more than 3 persons when it disposes documents, diskettes, storage media etc in relation to certification service.

5.1.5 Safe Operation of Back-Up Facility Located in Remote Place

CrossCert performs routine periodical backups of licensed certification authority's authorized certificates, critical storage media, subscriber's authorized certificates, authorized certificates suspension and revocation list etc and it stores in the remote area located more than 10 Km far from the certification center for 10 years in order to protect from fires or floods and it stores authorized certificates suspension and revocation list etc for 10 years from the commencement date the authorized certificates became ineffective.

5.2 Procedural Protective Measures

5.2.1 Task Allocation and Responsible Personnel on Licensed Certification Work

CrossCert's alloction of the relevant tasks in relation to certification work and responsible persons are as the followings.

< Tasks in relation to Certification Work and Responsible Persons>

Person in Charge	Tasks
Head of Certification Business Department	- General Managing Licensed Certification Center
Center Operating Manager	- Operating Management of Licensed Certification Center
Key Creation/Policy Manager	- Creating Digital Signature Key of Licensed Certification Center - Policy Management on Authorized Certificate Creating System
Security/Audit Manager	- Managing Security and Audit for Licensed Certification Center - Preventing Invasion, Detecting Invasion, Auditing Management for Access Control System - Managing Keys of Licensed Certification Center - Audit Managing on Digital Signature Key Creation - Audit Managing on Time-Stamping System
Licensed Certification System Operation/Manager	- Managing Operation of Authorized Certificate Creating System - Managing Operation of Directory System Works - Managing Operation of OCSP System - Managing Operation of Time-Stamping System Works - Managing Operation of Registration Management System - Managing Operation of Web Server - Managing Operation of Preventing Invasion, Detecting Invasion, Access Control System - Managing Operation of Other Relevant System to Licensed Certification Service
Safe Manager	- Managing Passwords of Safe
Manager of Safe Key	- Managing Key of Safe

5.2.2 Verification Methods on Responsible Personnel of Licensed Certification Work

CrossCert verifies the identity charging the certification work by ascertaining the ID card, finger print, password of each personnel.

5.2.3 Licensed Certification Work Which Can Not be Performed Simultaneously by the Same Person

CrossCert shall prevent the following tasks from being done by the same person according to the digital signature certification practice statement.

- When CrossCert creates its digital signature key (More than 3 Persons)
- When CrossCert creates the applicant's digital signature key (More than 2 Persons)
- When CrossCert installs, operates, maintains, and repairs the following systems (More than 2 Persons)
  - System supporting the functions on managing the registered information of subscriber
  - System supporting the functions of creation, issuance, and management of authorized certificates
  - System supporting the functions of time-stamping

CrossCert physically and logically destroys the storage media having the digital signature creating key to make it impossible to recovery under the attendance of more than 3 persons when the validity period of authorized certificates expired or the digital signature creating key becomes damaged or leaked.

5.3 Technical Protective Measures

5.3.1 Issues Regarding Protection of Digital Signature Creating Key

Digital signature key generating system is independently operated without the connection to the internal and external parts of the information telecommunication networks. Digital signature key generating system is operated and protected from physical invasion with equipped by multiple access controlling methods, which it is allowing the authorized person only to access to the system and generate the digital signature key pair and request form for authorized certificates

CrossCert generates the digital signature key by using KCDSA or RSA digital signature algorithm that having more than 1024 bit of its size for the use of safety confirmed and reliable digital signature algorithm and it makes use of HAS-160 or SHA-1 hash algorithm in order to generate more than 160 bit in its hash value.

CrossCert stores the digital signature creating key after sealing and encryption into the storage

device that is equipped with the functions of the access authority verification and leak or changes prevention of the digital signature creating key in order to safely store and manage the digital signature creating key generated in the digital signature key generating system.

Digital signature key generating system deletes the digital signature key from the memory of the system immediately after generating and saving it into the digital signature creating key storage device and then reboots the system.

CrossCert uses the digital signature creating key for the use of licensed certification authority only to the extent that the authorized certificate in question is valid.

5.3.2 Issues Regarding Protection for Composition and Management of Licensed Certification System etc.

CrossCert composed its core certification system and major systems relating to the certification service operation into the double structures and the certification service may be continuously provided by using the back-up system even if system failures make impossible to provide the certification service. The composed network lines are designed to be provided from the different ISP by duplexing, therefore if it occurs in one network line, the telecommunication traffic will be automatically transmitted into the other line.

5.3.3 Issues Regarding Configuration Management of Licensed Certification Software etc.

CrossCert shall perform the configuration management for the following facility and equipment according to the digital signature certification practice statement.

- Authorized certification system and subscriber software
- Network components and equipments
- Network safety operation system and server management system
- Access control relating system
- Other operation system

CrossCert shall manage the digital signature or hash value that is capable of guaranteeing the integrity of the software when it distributes the subscriber software.

5.3.4 Issues Regarding Protection for Composition and Operation of Network etc.

CrossCert uses the firewall system that has been received the test approved as K4 level from

Korea Internet & Security Agency in order to prevent illegal invasion and disclosure through in/external network, and it installs and operates the invasion detection system in order to detect the invasion into all of the core certification system and certification operation relating system, including authorized certificate generating management system, OCSP system, directory system, time-stamping system (hereinafter, "Core Certification System").

5.3.5 Protective Measures on Additional Services including Time-Stamping etc.

① Time Source

CrossCert uses the safe and reliable timing source by adopting the atomic clock and the satellite reception device etc. for the time-stamping service and it further uses the continuous time-adjusting functions thereof.

② System Duplex

CrossCert installs and operates the system in duplex for operating the additional services with equipped by the same functions.

③ System Access Control

CrossCert controls the access to the additional service operating system in order to prevent from the forgery of software and threat to forge the system, so that the duly authorized person only can access to the afore-mentioned system.

④ Audit Records of System

CrossCert audits, writes, and stores the records in relation to the operationg matters for providing the additional services.

⑤ Access Control to Audit Records

CrossCert controls the access to the additional service operating system in order to prevent from the forgery/fraudulent change of audit records and threat to delete the audit records, so that the duly authorized person only can access to the afore-mentioned audit records.

5.4 Personnel Security

5.4.1 Qualifications, Experience etc Requirements and Background Check Procedures on Responsible Personnel of Licensed Certification Work

CrossCert closely conducts the identity verification and background checks on all of its employees

and officers those who are dealing with the works relevant to authorized certification services, accessing to authorized certification center and the certification system, as a result only the employees/officers those who are duly approved may perform the duties related to certification and security work.

Qualifications and experiences of employees/officers those who are eligible to be assigned to authorized certification related work shall be correspondingly applied as stated in Article 3 (Appointment Standards) in Enforcement Decree of the Act. A person who comes under Article 5 (Reasons for Disqualification) of the Act shall not be assigned to the work in relation to the certification system.

5.4.2 Training Licensed Certification Work and Job Rotation

CrossCert has separated the certification work by respective system and function for the safe operation, so it enables each employee performs the different duties. If one employee performs various certification tasks, the employee shall not connect those tasks each other.

Responsible manager of CrossCert shall have its personnel complete the requisite education according to the attached Table 4 (Other Measures for stability of the Facilities Regarding Certification Work) of Rules on Protective Measures of Licensed Certification Authority.

5.4.3 Sanctions for Unauthorized Actions

CrossCert takes the appropriate disciplinary actions for unauthorized actions according to Article 31 and Article 32 (Penalty Clause) of the Act and penalty clauses in the Act on the Protection of Information and Communications Infrastructure if their personnel who perform certification work have done unauthorized actions by the digital signature laws and this Certification Practice Statement. Apart from the foregoing, CrossCert imposes the disciplinary sanctions on the said violator.

5.5 Audit Record

5.5.1 Types of Audited Records and Retention Period

CrossCert records the details of the following facts (or events) and the relevant time and details on the relevant people into the audit record files and it retains them.

- Facts that it has input/accessed/changed/deleted subscriber's registered information
- Facts that it has registered and managed subscriber's authorized certificate etc.
- Facts that it has added and deleted the account
- Facts that it has logged-in and loggged-off
- Facts that user's authority has been changed
- Facts that it has created/issued/renewed/suspended or revoked authorized certificates
- Facts that it has generated/accessed/disposed of the digital signature key
- Facts that it has time-stamped the electronic documents
- Facts that it has activated/suspended the core certification system
- Facts of other major activities of the core certification system manager

CrossCert examines the normality in the records relevant to the operation of the authorized certification work according to Article 27(Management of Audit Records) of Guides on Digital Signature Certification Work and the records generated from the certification system.

5.5.2 Protective Measures, Back-Up Period, and Procedure for Audited Records

CrossCert appoints 2 employees as (Main/Assistant) Audit Manager and Audit Manager examines the audit records once a day and preserve it according to rules on records archival and back-up as stated in 5.6 of this Certification Practice Statement.

General management on the audit records of each system shall be conducted by (Main/Assistant) Audit Manager and the respective worker of each system may read the audit records related to its own work only.

5.6 Records Archival

5.6.1 Types of Records Archived and Retention Period

CrossCert shall retain the following records according to Article 22 (Keeping Records of Certification Work) of the Act while it performs the core certification work and it shall comply with Article 25 of Guideline on Digital Signature Certification Work.

- Basic information submitted when subscriber and user receives authorized certificates
- Details of Restriction made by physical and procedural controls
- General matters on certification work from the issuance of authorized certificate, to the revocation, suspension, and recovery of authorized certificate.

- Various audit records under the operation of the core certification system and operation details of operator
- Other policy matters determined as necessary to be recorded at CrossCert's discretion

It is the principle that the record needs to be retained under this section shall be retained for a period of 10 years after the termination of the validity of the certificates concerned by keeping 2 copies (i.e. the original copy and the duplicated copy) regularly.

5.6.2 Protective Measures on Records Archived

CrossCert protects the archive with keeping the security through the physical and procedural personnel controls, and it restricts the manager's scope of work through the personnel control and stores in the cabinet equipped with the locking device, which it protects against the modification/tampering/and damaging thereof.

5.6.3 Back-Up Period and Procedure for Records Archived

CrossCert backs up the records archived into the storage facility located in the remote site in preparation for the loss and destroy of the records in case of a natural disaster or an incident.

5.7 Failure Restoration and Disaster Recovery

5.7.1 Report and Recovery Procedure upon the Occurrence of Impediments and Disastrous Incidents on Licensed Certification Work

If the obstacles and damages are occurred to the system source and software etc., CrossCert conducts the recovery from the obstacles without delay by using the system source and software.

If the damages/destroy has been occurred to the major data including subscriber's authorized certificates, CrossCert recovers by using the backed up and achieved records without delay.

In the event that the security incident occurs, the respective system operators should report it to the manager in charge of the task by using the invasion detection system's automatic alarming functions etc.

5.7.2 Assuring Plan for Continuity Capabilities including Prevention of Occurrence of Obstacles to Licensed Certification Work

CrossCert exerts its efforts to provide the stable authorized certification service in the compliance with Article 19 (Operation of Certification Work System) of the Act and Article 13-5 (Regular Inspection) of the Rules of the Act.

CrossCert conducts the self-prepared vulnerability assessments once a month in the regular basis in order to seek for the effective security control methods upon the change of the system operation and it conducts the special assessments each quarter on a rolling basis and once a year.

CrossCert archives the audit record, data relevant to authorized certification service, subscriber's authorized certificate etc. in the regular basis into the back up facilities and it retains them in the safe that can be physically restricted to access.

Chapter 6. Warranties on Licensed Certification Work etc., Miscellaneous Matters

6.1 Warranties

6.1.1 Warranties on Licensed Certification Work and Disclaimers of Warranties

① Warranty

CrossCert warrants the following matters regarding the subscriber's authorized certificate that is issued by the creating key matched to the digital signature verifying key included in the licensed certification authority's authorized certificate issued by Korea Internet & Security Agency for CrossCert.

- The facts that there is no error in the contents included in the authorized certificate compare to the registered facts
- The facts that the contents in relation to the authorized certificate suspension and revocation list are not incorrect
- The facts that the authorized certificate has been issued in compliance with the digital signature relevant laws and the certification practice statement

② Limitation on Warranty

CrossCert does not warrant that an authorized certificate assures the credit ratings of the subscriber and user, invariability of the subscriber's information etc, which are matters other than prescribed in the above subsection. Therefore, the contents included in the authorized certificates

does not provide users any warranty of the subscriber's credit and identity information and fitness for a particular purpose or user's specific work.

6.2 Liability

6.2.1 Compensation Policy in Relation to Licensed Certification Service

CrossCert compensates for the loss and damages incurred to the subscriber or the user who trusted the authorized certificate in connection with the performance of the certification work according to Article 26 of the Act.

CrossCert shall subscribe for insurance in order to compensate the damages incurred to the subscriber or the user who trusted the authorized certificate in connection with the performance of the certification work.

The compensation responsibility for damages applies to all kinds of damages and losses and the compensation shall be made to the subscriber or user who has the justifiable reasons for the compensation, provided the maximum amount for compensation is limited to KRW 500,000,000 in each case.

6.2.2 Limitations of Liability by the Insurance CrossCert subscribed

CrossCert shall assume the liability for compensation by the insurance to the extent of KRW 2,000,000,000 in total compensation amount for each authorized certificate issued by CrossCert per year.

The limited amount for compensation by insurance includes all of the damages incurred to all of the persons in relation to the authorized certificates issued, managed, revoked, suspended, expired by CrossCert. Any compensation liability exceeding the limited amount by insurance shall be agreed between the parties or determined by the court's judgment.

6.2.3 Indemnities

CrossCert shall not be responsible for the following matters that are incurred to the subscriber, user, and registration authority etc, nevertheless CrossCert complied with the digital signature relating laws and certification practice statement of Korea Internet & Security Agency and it abided by responsibilities and obligations prescribed in this certification practice statement.

- Other losses incurred to subscriber and user due to the following causes in connection with the performance of the authorized certification service
  - Responsibility and obligation undefined in the certification practice statement
  - Inaccurate information except for prescribed matters in the certification practice statement
  - Responsibility for user's recklessness and ignorance
  - Integrity, newness, fitness for specific purpose, etc. of information included in the authorized certificate

- Loss or damages resulted from the subscriber and user ignored or omitted taking necessary actions, nevertheless it has been notified through the certification practice statement and the notice board in its web-site etc. regarding the possibility of occurrence of the problems.
- Non-repudiation on the facts of transmission and reception in relation to transmitted/received electronic documents. Provided, it is possible to confirm and create the supportive source for non-repudiation

In addition, it shall not be responsible for the damages incurred to subscriber and user due to the following reasons other than faults/defects of licensed certification authority or authorized certificate.

- Loss resulted from non-performance of the obligations by subscriber and user
- Obstacles not in CrossCert's system but in the telecommunication network lines during the performance of certification service
- Loss by the use of the expired authorized certificate
- Loss exceeding the prescribed scope of loss in the digital signature relating laws and certification practice statement of Korea Internet & Security Agency and this certification practice statement
- Loss by the use of the suspended or revoked authorized certificate
- Loss incurred to subscriber and user due to the delay and cessation of the certification service resulted from the defects of software or hardware that is not provided by CrossCert
- Certification service is not provided due to the occurrence of war or other natural disaster etc. or force majeure events
- It is not an incident caused by CrossCert's negligence or misconduct

6.3 Dispute Resolution

6.3.1 Requirements for Having Legal Validity on the Document Transmitted to a Relevant Party of Digital Signature Certification System

In order for the document transmitted to the relevant persons in the certification system to have the legal validity, there should exist the digital signature verified by the licensed certification authority in compliance with the digital signature relating laws and certification practice statement of Korea Internet & Security Agency and this certification practice statement.

6.3.2 Interpretation of Certification Practice Statement and Governing Law in Relation to Enforcement

This certification practice statement is interpreted and governed by the relevant laws of Republic of Korea.

6.3.3 Competent Court for Legal Proceedings

If any dispute arises in association with the certification work between CrossCert and subscriber or user, all legal proceedings for the dispute resolution shall be bound by the clauses on 'jurisdiction' in the Civil Procedure Act.

6.3.4 Dispute Resolution Procedure

Ministry of Public Administration etc, the relevant governmental authority and Korea Internet & Security Agency may arrange the dispute to the conciliation according to the digital signature relating laws and other relevant laws with the fastest methods after reviewing the existence of a breaching conduct of the digital signature relating laws and the compliance with the certification practice statement.

If there is a dispute between subscriber and user, CrossCert may request the relevant parties to submit the document concerned and assesses whether they complied with the digital signature relating laws and the certification practice statement, and then offer a draft for the conciliation and recommend reaching an agreement. At the time, the relevant parties or initiator of the dispute requests for the assessment in a written document to CrossCert and the document shall be delivered to the relevant parties.

CrossCert may request for the dispute settlement to Korea Internet & Security Agency if a dispute occurs. In this case, CrossCert may request the relevant parties to submit the document concerned and assesses whether they complied with the digital signature relating laws and the

certification practice statement, and then offer a draft for the conciliation and recommend reaching an agreement.

6.4 Privacy of Personal Information

6.4.1 Policy on Privacy of Personal Information

CrossCert and registration authority collects the subscriber's information to the minimum extent for the performance of its certification work, according to the digital signature relating laws and the Acts on Information Telecommunication Network Usage Promotion and Information Protection, and it collects the distinguishable information of subscriber under the consent by the subscriber. Provided subscriber's information shall not be disclosed to a third party or used any other purpose without the subscriber's own consent, further CrossCert and registration authority shall be responsible for the foregoing. Provided however the followings are the exceptions.

- It is necessary for the settlement of fees
- There is a specific provision in law/regulation
- Providing indistinguishable forms of information and it is the case for statistics, academic research, or market research purposes

When CrossCert and registration authority receives consent from the subscriber, they shall notify the identity of the responsible personnel for subscriber's information management (name, department, position and telephone no, other contact information), the purpose of information collection, information on providing the information to a third party (receiver, purpose of provision and contents of providing information) etc as stated in Article 22.2 of the Acts on Information Telecommunication Network Usage Promotion and Information Protection, which the subscriber may withdraw his/her consent at any time.

Subscriber may request for reading, error correction, deleting of his/her own information that CrossCert and registration authority hold at any time, in response CrossCert shall take necessary measures without delay. If the subscriber requests for the correction of errors, CrossCert and registration authority must not use the subscriber's information until the error is corrected. CrossCert and registration authority shall minimize the number of the relevant manager and assumes all of the liability for damages incurred due to the stealth, missing, leak, tampering etc of the subscriber's information.

CrossCert and registration authority or the third party who received the subscriber's information

from CrossCert or registration authority shall destroy the subscriber's information without delay once it is achieved the purpose of the receipt of the subscriber's information.

6.5 Inspection and Check-up etc.

CrossCert receives the check-ups on its facilities in relation to certification work and whether it is safely operated in the regular period in order to ensure the safety of the certification related facilities according to Article 13-5 (Regular Inspection) of Enforcement Rule of the Act.

The items for the afore-mentioned regular inspection include items whether CrossCert complies with this Certification Practice Statement and items whether it is taking 'protective measures for ensuring the safety of the certification work related facilities' according to Article 13-4 of Enforcement Rule of the Act.

6.6 Compliance with Applicable Law

This Certification Practice Statement complies with the Act, Enforcement Decree of the Act, Enforcement Rule of the Act and Certification Practice Statement of Korea Internet & Security Agency.

6.7 Effectiveness of Certification Practice Statement

6.7.1 Effective Date

This Certification Practice Statement is effective from July 21, 2007.

6.7.2 Conditions for Termination of Certification Practice Statement

This Certification Practice Statement becomes void when CrossCert closes the certification work according to the digital signature relating laws or it cannot provide certification work due to a cause prescribed in Article 12 (Suspension of Certification Work or Revocation of Designation, etc.) of the Act.