DIGITAL SIGNATURE ACT

Act No. 5792, Feb. 5, 1999
Amended by Act No. 6360, Jan. 16, 2001
Act No. 6585, Dec. 31, 2001
Act No. 7428, Mar. 31, 2005
Act No. 7813, Dec. 30,2005
Act No. 8852, Feb. 29, 2008
Act No. 9208, Dec. 26, 2008

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Act is to establish the basic framework for the system of digital signatures in order to secure the safety and reliability of electronic messages and to promote their use, thereby stimulating the use of electronic records and communications on a national level and advancing social benefit and convenience.

Article 2 (Definitions)

The terms used in this Act shall be defined as follows:

1. The term "electronic message" means a piece of information generated and sent, received, or stored in a digital form through information processing system;
2. The term "digital signature" means a piece of information in a digital form affixed on, or logically combined to, an electronic message in order to identify the signer and verify that the electronic message has been signed by that signer;
3. The term "certified digital signature" means a digital signature that satisfies the following requirements and is grounded upon an authorized certificate:
   (a) That the digital signature creating key shall be held and known only by the subscriber;
   (b) That the subscriber shall hold and keep control of the digital signature creating key at the time of signing;

(c) That it shall be able to be ascertained whether there has been any alteration in the digital signature concerned since it was affixed; and

(d) That it shall be able to be ascertained whether there has been any alteration in the electronic message concerned since digital signature was affixed;

4. The term "digital signature creating key" means a sequence of bits used to affix a digital signature to an electronic message;
5. The term "digital signature verifying key" means a sequence of bits used to verify a digital signature;
6. The term "certification" means the act of ascertaining and verifying that the digital signature creating key is held and known only by the subscriber;
7. The "certificate" means a computer-based record ascertaining and verifying that the digital signature creating key is held and known only by the subscriber;
8. The term "authorized certificate" means a certificate that a licensed certification authority issues in accordance with Article 15;
9. The term "authorized certification work" means the affairs of offering authorized certification services, such as the issuance of authorized certificates, the maintenance of certification-related records, etc.;
10. The term "licensed certification authority" means an entity that is, in accordance with Article 4, designated as such in order to offer authorized certification services;
11. The term "subscriber" means a person whose digital signature creating key has been certified by a licensed certification authority;
12. The term "signer" means a person who holds his own digital signature creating key and signs in his own name or on behalf of another person; and
13. The term "information on individual" means a piece of information that pertains to a living individual, which is such marks, letters, voice, sound, image, physical characteristics, etc. as may serve to establish the identity of the person concerned with the help of name, resident registration number, etc. (including such information as may, even if this information is short of identifying a specific person, combine easily with other information to establish his identity).

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 3 (Effect, etc., of Digital Signature)

(1) In cases that a signature, signature and seal, or name and seal is, under other Acts and subordinate statutes, required to be affixed on a paper-based document or letter, it shall be deemed that such requirements are satisfied if there is a certified digital signature affixed on an electronic message. *<Amended by Act No. 6585, Dec. 31, 2001>*

(2) In cases that a certified digital signature is affixed on an electronic message, it shall be presumed that such a digital signature is the signature, signature and seal, or name and seal of the signer of the electronic message concerned and that there has been no alteration in the contents of such message since it was signed digitally. *<Amended by Act No. 6585, Dec. 31, 2001>*

(3) A digital signature other than a certified digital signature shall have such an effect of a signature, signature and seal, or name and seal, as is agreed between the parties concerned. *<Newly Inserted by Act No. 6585, Dec. 31, 2001>*

CHAPTER II LICENSED CERTIFICATION AUTHORITY

Article 4 (Designation of Licensed Certification Authority)

(1) The Minister of Public Administration and Security may designate as a licensed certification authority an entity that is deemed to be capable of performing authorized certification work (hereinafter referred to as "certification work") in a secure and reliable manner. *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 8852, Feb. 29, 2008>*

(2) The entity that can be designated as a licensed certification authority shall be limited to State agencies, local governments and corporations.

(3) The entity that desires to be designated as a licensed certification authority shall meet such requirements as technical and financial capabilities, facilities and equipment, and other required matters as provided by the Presidential Decree.

(4) Where the Minister of Public Administration and Security designates a licensed certification authority under paragraph (1), he/she may designate it, for a sound development, etc. of the authorized certification market,

by dividing the domain of certification work under the establishment purpose in case of State agencies, local governments, non-profit corporations or corporations established by special Acts. <*Newly Inserted by Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008*>

(5) Procedures for designation of a licensed certification authority and other necessary matters shall be determined by the Presidential Decree.

Article 5 (Disqualification)

No entity that falls under any of the following subparagraphs shall be designated as a licensed certification authority: <*Amended by Act No. 7428, Mar. 31, 2005*>

1. A corporation of which any officer falls under any of the following items:
   (a) A person who has been declared by a court as incompetent, quasi-incompetent or bankrupt and remains not reinstated;
   (b) A person in whose case two years have not yet passed since his/her imprisonment without prison labor or heavier punishment as declared by a court was completely executed (including the case where it is deemed to have completely been executed) or exempted from being executed;
   (c) A person who is under suspension of the execution of imprisonment without prison labor or heavier punishment as declared by a court;
   (d) A person who has been disqualified or whose qualification has been suspended by the court decision or under other Acts; and
   (e) A person who was in the position of an officer of a corporation at the time when its designation as a licensed certification authority was revoked pursuant to Article 12 (limited to a case where two years have not yet passed since its revocation); and
2. A corporation in whose case two years have not yet passed since its designation as a licensed certification authority was revoked pursuant to Article 12.

Article 6 (Rules, etc. of Authorized Certification Work)

(1) A licensed certification authority shall make its rules of authorized certification work (hereinafter referred to as the "rules of certification work") that contains matters set forth in each of the following subparagraphs and report them to the Minister of Public Administration and Security before

it begins to perform certification work: *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

1. Categories of certification work;
2. Method and procedures for performing certification work;
3. Utilization terms of authorized certification services (hereinafter referred to as "certification services"); and
4. Such other matters as may be necessary for carrying out certification work.

(2) A licensed certification authority shall prepare the rules of certification work under the preparation standard for the rules of authorized certification work and the digital signature certification work guidelines under the provisions of Article 8 that are provided and publicly announced by the Minister of Public Administration and Security. *<Newly Inserted by Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

(3) In case of the modification of the matters already reported under paragraph (1), a licensed certification authority shall report to the Minister of Public Administration and Security thereof within a period of time as prescribed by Ordinance of the Ministry of Public Administration and Security. *<Newly Inserted by Act No. 6585, Dec. 31, 2001; Act No. 8852, Feb. 29, 2008>*

(4) Where the contents of rules of certification work reported under the provisions of paragraph (1) for the securing of safety and reliability of certification work and for the protection of subscribers' interests violate the preparation standard for the rules of authorized certification work provided and publicly announced by the Minister of Public Administration and Security and the digital signature certification work guidelines under the provisions of Article 8 (1), the Minister of Public Administration and Security may order the licensed certification authority concerned to modify the same rules of certification work within a reasonable and fixed period of time. *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

(5) A licensed certification authority shall faithfully observe all the matters as prescribed by the rules of certification work. *<Newly Inserted by Act No. 6585, Dec. 31, 2001>*

Article 7 (Provision, etc. of Certification Services)

(1) No licensed certification authority shall refuse to provide certification services without any justifiable reason.

(2) No licensed certification authority shall unjustly discriminate against a subscriber or a certification service user.

Article 8 (Performance of Certification Work by Licensed Certification Authority)

(1) In order to secure the safety and reliability of certification work, the Minister of Public Administration and Security may draw up and publicly announce digital signature certification work guidelines on such definite matters as shall be observed by a licensed certification authority in performing certification work. *<Amended by Act No. 8852, Feb. 29, 2008>*

(2) The digital signature certification work guidelines under paragraph (1) shall contain the matters of the following subparagraphs: *<Newly Inserted by Act No. 7813, Dec. 30, 2005>*

1. Matters concerning the management of authorized certificates;
2. Matters concerning the management of digital signature creating keys;
3. Matters concerning the protection of the facilities of licensed certification authorities; and
4. Other matters concerning the certification work and operational management.

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 9 (Acquisition of Certification Work by Transfer, etc.)

(1) A licensed certification authority, which desires to acquire the certification work of another licensed certification authority or to merge with another licensed certification authority that is a corporation, shall report to the Minister of Public Administration and Security thereof as prescribed by Ordinance of the Ministry of Public Administration and Security. *<Amended by Act No. 8852, Feb. 29, 2008>*

(2) A licensed certification authority that has acquired the certification work as referred to in paragraph (1), or in the case of merger, the corporation that has survived or newly been established after the merger thereunder shall succeed to the status of the former licensed certification authority.

Article 10 (Cessation, Closure, etc. of Certification Work)

(1) When a licensed certification authority desires to cease all or part of its certification work, it shall fix the period of cessation and notify its subscribers thereof not later than 30 days before the scheduled date of cessation, and also report to the Minister of Public Administration and

Security thereof. In such cases, this period of cessation shall not exceed six months. <*Amended by Act No. 8852, Feb. 29, 2008*>

(2) When a licensed certification authority desires to close its certification work, it shall notify its subscribers thereof not later than 60 days before the scheduled date of closure, and also report to the Minister of Public Administration and Security thereof. <*Amended by Act No. 8852, Feb. 29, 2008*>

(3) The licensed certification authority that has reported under paragraph (2) shall transfer to another licensed certification authority its subscriber's authorized certificates as well as the records of the authorized certificates the validity of which was suspended and which was revoked (hereinafter referred to as the "subscriber's certificates, etc."): *Provided*, That if the subscriber's certificates, etc. may not be transferred to another licensed certification authority due to unavoidable circumstances, the licensed certification authority shall, without delay, report such a fact to the Minister of Public Administration and Security. <*Amended by Act No. 6585, Dec. 31, 2001; Act No. 8852, Feb. 29, 2008*>

(4) Upon receipt of the report under the proviso of paragraph (3), the Minister of Public Administration and Security may order the Korea Information Security Agency under Article 52 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as the "Information Security Agency") to take over the subscriber's certificates, etc. from the licensed certification authority concerned. <*Amended by Act No. 6360, Jan. 16, 2001; Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008*>

(5) Such matters as may be necessary for the report of the cessation or closure of certification work as well as the transfer and takeover of the subscriber's certificates, etc. as referred to in paragraphs (1) through (4) shall be prescribed by Ordinance of the Ministry of Public Administration and Security. <*Amended by Act No. 8852, Feb. 29, 2008*>

Article 11 (Corrective Order)

The Minister of Public Administration and Security may order a licensed certification authority to take corrective measures within a fixed period of time if it falls under any of the following subparagraphs: <*Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008*>

1. Deleted; <*by Act No. 7813, Dec. 30, 2005*>
2. Where a licensed certification authority fails to satisfy the require-

ments it should meet under Article 4 (3) after it was designated as a licensed certification authority;

3. Where an officer of a licensed certification authority falls under any of the items of subparagraph 1 of Article 5;
4. Where a licensed certification authority fails to make a report or a report of alterations under Article 6 or where it fails to observe its rules of certification work that have been reported thereunder;
5. Where a licensed certification authority refuses to provide certification services, or unjustly discriminates against subscribers or certification service users, in violation of Article 7;

5-2. Where a licensed certification authority fails to observe such definite matters as determined in the digital signature certification work guidelines, in violation of Article 8;

6. Where no report is made on the acquisition of a certification work by transfer, or on a merger between the licensed certification authorities, in violation of Article 9 (1);
7. Where a licensed certification authority fails to give notice of, or to make report on, the cessation or closure of its certification work, or where it fails to transfer its subscriber's certificates, etc. to another certification authority at the time of the closure of its certification work, in violation of Article 10;
8. Where a licensed certification authority, the designation of which is revoked, fails to transfer its subscriber's certificates, etc. to another certification authority, or fails to make a report it is required to do in case of no transfer, in violation of Article 12 (2);
9. Where documents and materials as referred to in Article 14 (1) are not submitted;

9-2. Where a licensed certification authority fails to confirm the identity under the latter parts of Article 15 (1);

10. Where a licensed certification authority fails to suspend or restore the validity of an authorized certificate, or where it fails to take such measures as may be necessary for this information to be at all times accessible to the public, in violation of Article 17;
11. Where a licensed certification authority fails to revoke an authorized certificate, or where it fails to take such measures as may be necessary for this information to be at all times accessible to the public,

in violation of Article 18;

11-2. Where a licensed certification authority fails to take protective measures to secure the safety of certification work facilities in violation of Article 18-3;

12. Where a licensed certification authority fails to report on an occurrence of obstacles to the information processing systems providing a certification work under the provisions of Article 22-3 (1); and

13. Where a licensed certification authority fails to subscribe to the insurance under the provisions of Article 26 (2).

Article 12 (Suspension of Certification Work or Revocation of Designation, etc.)

(1) Where a licensed certification authority falls under any of the following subparagraphs, the Minister of Public Administration and Security may suspend all or part of its certification work for a fixed period not exceeding 6 months, or revoke its designation as a licensed certification authority: *Provided*, That in such cases as set forth in subparagraphs 1 and 2, its designation shall be revoked: *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

1. Where a designation as provided in Article 4 was obtained through fraud or any other wrongful means;
2. Where a licensed certification authority which has been ordered to suspend its certification work fails to suspend the certification work in violation of such an order;
3. Where certification work is not commenced within 6 months after designation as provided in Article 4 or where certification work is ceased for 6 or more consecutive months;
4. Where an order to alter the rules of certification work as provided in Article 6 (4) is violated; and
5. Where a corrective order as provided in Article 11 is not implemented without any justifiable reason.

(2) A licensed certification authority the designation of which is revoked pursuant to paragraph (1) shall transfer its subscriber's certificates, etc. to another licensed certification authority: *Provided*, That if the subscriber's certificates, etc. may not be transferred due to an inevitable circumstances, the licensed certification authority shall, without delay, report it to the Minister of Public Administration and Security. *<Amended*

by Act No. 8852, Feb. 29, 2008>

(3) The provisions of Article 10 (4) shall apply *mutatis mutandis* to a licensed certification authority the designation of which is revoked.

(4) Necessary matters pertaining to standards and procedures for dispositions as referred to in paragraph (1) as well as transfer and takeover, etc. under paragraphs (2) and (3) shall be prescribed by Ordinance of the Ministry of Public Administration and Security. *<Amended by Act No. 8852, Feb. 29, 2008>*

Article 13 (Imposition of Penalty Surcharge)

(1) Where a suspension of certification work as a sanction against an offence falling under any of subparagraphs of Article 12 (1) may cause subscribers, etc. serious inconvenience or may be harmful to other public interests, the Minister of Public Administration and Security may impose a penalty surcharge not exceeding 20 million won, in lieu of that suspension of certification work. *<Amended by Act No. 8852, Feb. 29, 2008>*

(2) The amount of a penalty surcharge according to the types and nature of the offences subject to penalty surcharge under paragraph (1) and other necessary matters shall be determined by the Presidential Decree. *<Amended by Act No. 7813, Dec. 30, 2005>*

(3) When a person who is obligated to pay a penalty surcharge under paragraph (1) fails to do so by due date, the Minister of Public Administration and Security shall collect it by referring to the practices of dispositions on default of national taxes. *<Amended by Act No. 8852, Feb. 29, 2008>*

Article 14 (Inspection, etc.)

(1) In order to confirm the matters of the following subparagraphs for the securing of the safety and reliability of certification work, protection of subscribers, etc., the Minister of Public Administration and Security may order a licensed certification authority to submit the relevant documents and materials, and direct the relevant public official to enter its office, work site, or any other necessary premises to inspect facilities, equipment, books, records and other items concerning certification work: *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

1. Whether or not the procedures and methods for an identity confirmation by a licensed certification authority under the provisions of Article 15 are appropriate; and
2. Whether or not the safety and reliability of confirmation work provided

in the provisions of Articles 18-3, 19 through 22, 22-2, 23 and 24 are secured.

(2) Where the Minister of Public Administration and Security has the relevant public official inspect under the provisions of paragraph (1), he/she shall notify the relevant licensed certification authority of the inspection plans for date, reasons and details of inspection, not later than 7 days before the beginning of inspection. *<Newly Inserted by Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

(3) The public official who enters to conduct an inspection pursuant to paragraph (1) shall show a certificate verifying his/her authority to the interested persons, and deliver to the interested persons at the time of entry, the document indicating his/her name, time of entry and purpose of entry, etc. *<Amended by Act No. 7813, Dec. 30, 2005>*

CHAPTER Ⅲ AUTHORIZED CERTIFICATE

Article 15 (Issuance of Authorized Certificate)

(1) A licensed certification authority shall issue an authorized certificate to the person who applies for the issuance of an authorized certificate. In this case, the licensed certification authority shall verify the identity of the applicant. *<Amended by Act No. 6585, Dec. 31, 2001>*

(2) An authorized certificate issued by a licensed certification authority shall contain such particulars as set forth in the following subparagraphs: *<Amended by Act No. 6585, Dec. 31, 2001>*

1. Subscriber's name (in the case of a corporation, its name or trade name);
2. Subscriber's digital signature verifying key;
3. Description of algorithm used by the subscriber and the licensed certification authority to sign the authorized certificate;
4. Serial number of the authorized certificate;
5. Effective period of the authorized certificate;
6. Name of the licensed certification authority and other information that can serve to verify the identity of the licensed certification authority;
7. If there is any limit imposed on the scope or purposes of the use of the authorized certificate, matters pertaining thereto;

8. If the subscriber has the proxy, etc. to act for another or if he/she asks his/her professional title, etc. to be entered, matters pertaining thereto; and
9. A mark verifying the authorized certificate.

(3) Deleted. *<by Act No. 6585, Dec. 31, 2001>*

(4) If a person applies for the issuance of an authorized certificate, a licensed certification authority may issue an authorized certificate having limits on the scope or purposes of its use. *<Amended by Act No. 6585, Dec. 31, 2001>*

(5) A licensed certification authority shall give an appropriate period of validity to an authorized certificate, taking into account the scope or purposes of its use as well as the safety and reliability of the computing techniques used for its issuance. *<Amended by Act No. 6585, Dec. 31, 2001>*

(6) Necessary matters concerning the procedures and methods of verifying the identity of an applicant for the issuance of an authorized certificate shall be prescribed by Ordinance of the Ministry of Public Administration and Security. *<Newly Inserted by Act No. 6585, Dec. 31, 2001; Act No. 8852, Feb. 29, 2008>*

Article 16 (Termination, etc. of Validity of Authorized Certificate)

(1) Where there arise circumstances falling under any of the following subparagraphs, with respect to an authorized certificate issued by a licensed certification authority, the validity of that authorized certificate shall terminate at the time of the occurrence of such circumstances: *<Amended by Act No. 6360, Jan. 16, 2001; Act No. 6585, Dec. 31, 2001>*

1. Where the period of validity of an authorized certificate expires;
2. Where the designation of a licensed certification authority is revoked pursuant to Article 12 (1);
3. Where the validity of an authorized certificate is suspended pursuant to Article 17;
4. Where an authorized certificate is revoked pursuant to Article 18; and
5. Deleted. *<by Act No. 6585, Dec. 31, 2001>*

(2) Where the digital signature creating key of a licensed certification authority, whose certification work was ceased or closed under the provisions of Article 10 or suspended under the provisions of Article 12, has been lost, damaged, or stolen and outflowed, etc., the Minister of Public Administration and Security may, for securing the safety and reliability

of certification work, suspend the validity of all authorized certificates issued by the relevant licensed certification authority. *<Amended by Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

(3) When the Minister of Public Administration and Security has suspended the validity of authorized certificates pursuant to paragraph (2), he/she shall instruct the Information Security Agency to take without delay such measures as may be necessary for this information to be at all times accessible to the public. The same shall also apply to a case where the validity of authorized certificates terminates pursuant to paragraph (1) 2. *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 8852, Feb. 29, 2008>*

Article 17 (Suspension, etc. of Validity of Authorized Certificate)

(1) If there is a request on the part of a subscriber or his/her agent, a licensed certification authority shall suspend the validity of an authorized certif- icate or restore it by terminating the suspension. In this case, the request for the restoration of its validity shall be made within 6 months from the date on which the validity of the authorized certificate was suspended. *<Amended by Act No. 6585, Dec. 31, 2001>*

(2) In case that a licensed certification authority has suspended or re- stored the validity of an authorized certificate under paragraph (1), it shall, without delay, adopt such measures as may be necessary for this information to be at all times accessible to the public. *<Amended by Act No. 6585, Dec. 31, 2001>*

Article 18 (Revocation of Authorized Certificate)

(1) In cases that there arise circumstances falling under any of the fol- lowing subparagraphs with respect to an authorized certificate, the li- censed certification authority shall revoke this certificate: *<Amended by Act No. 6585, Dec. 31, 2001>*

1. Where a subscriber or his/her agent requests the revocation of an au- thorized certificate;
2. Where the licensed certification authority becomes aware that a sub- scriber has been issued an authorized certificate by fraud or other wrongful methods;
3. Where the licensed certification authority becomes aware that a sub- scriber has died or has been in disappearance as declared by a court, or that a subscriber as a corporation has been dissolved; or
4. Where the licensed certification authority becomes aware that a

subscriber's digital signature creating key has been lost, hacked, stolen or disclosed to a third party.

(2) In case that a licensed certification authority has revoked an authorized certificate pursuant to paragraph (1), it shall, without delay, take such measures as may be necessary for this information to be at all times accessible to the public. *<Amended by Act No. 6585, Dec. 31, 2001>*

Article 18-2 (Personal Identification by Authorized Certificate)

A person may identify himself/herself by means of an authorized certificate issued by a licensed certification authority under this Act unless the act of identifying a person himself/herself by such means is restricted or precluded by any other Act.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

CHAPTER Ⅳ SECURING OF SAFETY AND RELIABILITY OF CERTIFICATION WORK

Article 18-3 (Securing Safety of Licensed Certification Authority)

A licensed certification authority shall take protective measures prescribed by Ordinance of the Ministry of Public Administration and Security to secure the safety of facilities for performing certification work. *<Amended by Act No. 8852, Feb. 29, 2008>*

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 19 (Operation of Certification Work System)

(1) A licensed certification authority shall securely operate its facilities and equipment for performing certification work, including a certification work system that serves to enable the public to ascertain at all times whether the authorized certificates it issues remain valid.

(2) A licensed certification authority shall be subject to a regular inspection by the Information Security Agency to ascertain whether its facilities and equipment as provided in paragraph (1) are securely operated.

(3) Where a licensed certification authority replaces the facilities and equipment as provided in paragraph (1) after it was designated as such, it shall, without delay, report to the Minister of Public Administration and Security thereof. In such cases, the Minister of Public Administration

and Security may direct the Information Security Agency to inspect the new facilities and equipment in question for any problems in their safety.<*Amended by Act No. 8852, Feb. 29, 2008*>

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 20 (Time-Stamp of Electronic Messages)

A licensed certification authority may stamp by an authorized digital signature the time at which an electronic message is presented for its certification, if there is any request therefor on the part of a subscriber or an authorized certificate user (hereinafter referred to as the "user"). <*Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005*>

Article 21 (Control of Digital Signature Creating Key)

(1) A subscriber shall hold and keep control of his/her digital signature creat- ing key in a secure and confidential manner, and, when he/she becomes aware that it has been lost, hacked, stolen, or disclosed to a third person or that it is in danger of being likely to be hacked, he/she shall notify the licensed certification authority thereof. In this case, the subscriber shall, without delay, inform the users of the contents of the said notification he/she has sent to the licensed certification authority.

(2) A licensed certification authority shall provide its subscribers with the computational device by which they can inform or notify such facts as referred to in paragraph (1).

(3) A licensed certification authority shall not hold a subscriber's digital signature creating key unless the subscriber so requests; notwithstand- ing, if by the request of a subscriber it holds his/her digital signature creat- ing key, it shall not use or disclose the said key without the consent of the subscriber.

(4) A licensed certification authority shall hold and keep control of the digital signature creating key that it is using, in a secure and confidential manner. When it becomes aware that such a digital signature creating key has been lost, hacked, stolen or disclosed outside or that the digital signature creating key is in danger of being likely to be hacked, it shall, without delay, notify the Information Security Agency thereof and take such measures as to secure the safety and reliability of certification work.

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 22 (Keeping Records of Certification Work)

(1) A licensed certification authority shall keep and control records of the issuance of authorized certificates for its subscribers and the performance of its certification work in a secure manner. *<Amended by Act No. 6585, Dec. 31, 2001>*

(2) A licensed certification authority shall retain its subscriber's certificates, etc. for a period of 10 years after the termination of the validity of the certificates concerned. *<Amended by Act No. 6585, Dec. 31, 2001>*

Article 22-2 (Control, etc. of Authorized Certificates)

(1) A licensed certification authority and its subscriber shall pay due care in maintaining in a correct and perfect manner the contents of the authorized certificate concerned or the information associated with the authorized certificate while it remains valid.

(2) A licensed certification authority shall provide the users with such convenient device as to enable them to ascertain the matters set forth in the following subparagraphs by using the authorized certificate:

1. Name of the licensed certification authority and other information that can serve to verify the identity of the licensed certification authority;
2. The fact that the subscriber held and kept control of the digital signature creating key at the time of the issuance of the authorized certificate concerned; and
3. The fact that the digital signature creating key remained valid prior to the issuance of the authorized certificate.

(3) A licensed certification authority shall provide the users with such convenient device as to enable them to ascertain the matters set forth in the following subparagraphs:

1. Methods by which the identity of the signer can be verified;
2. Limits on the purpose of use of, or the amount permissible for, the digital signature creating key or the authorized certificate; and
3. The scope or limit of the liability incurred by the licensed certification authority.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 22-3 (Report on Occurrence of Obstacles to Certification Work)

(1) Where any obstacles have occurred to the information processing systems that provide the certification work, a licensed certification authority shall report such facts without delay to the Minister of Public Administration

and Security or the president of the Information Security Agency, and shall prepare the countermeasures capable of rapidly overcoming the obstacles. *<Amended by Act No. 8852, Feb. 29, 2008>*

(2) When the Minister of Public Administration and Security or the president of the Information Security Agency has received a report on obstacles to the certification work under the provisions of paragraph (1), he/she shall take the measures of the following subparagraphs: *<Amended by Act No. 8852, Feb. 29, 2008>*

1. Collection and dissemination of the information on obstacles; and
2. Technological support and cooperation concerning overcoming the obstacles.

[This Article Newly Inserted by Act No. 7813, Dec. 30, 2005]

Article 23 (Security of Digital Signature Creating Key, etc.)

(1) No person shall use by stealth or disclose another person's digital signature creating key. *<Amended by Act No. 6585, Dec. 31, 2001>*

(2) No person shall have an authorized certificate issued in the name of another person, or aid such issuance. *<Amended by Act No. 6585, Dec. 31, 2001>*

(3) No person shall use a similar mark that leads or may lead others to confuse an unauthorized certificate, etc. with an authorized certificate or shall falsely indicate the use of an authorized certificate. *<Newly Inserted by Act No. 6585, Dec. 31, 2001>*

(4) No person shall unlawfully use an authorized certificate by ridding oneself of the utilization scope or usage. *<Newly Inserted by Act No. 7813, Dec. 30, 2005>*

(5) No person shall transfer or rent an authorized certificate to other persons for the purpose of being exercised, or receive any transfer or rent of other persons' authorized certificate for the purpose of exercising. *<Newly Inserted by Act No. 7813, Dec. 30, 2005>*

Article 24 (Protection of Information on Individual)

(1) A licensed certification authority shall protect information on individual in connection with its performance of certification work.

(2) The provisions concerning the information on individual as referred to in Articles 22 through 32, 36 (1), 54, 55, 62, 66, and 67 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. shall apply *mutatis mutandis* to the protection of information on individual as provided in paragraph (1). In this

case, the "provider of information and communications service" shall be deemed to be "licensed certification authority" and "user" to be "subscriber". <*Amended by Act No. 7813, Dec. 30, 2005*>

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 25 (Digital Signature Certification Control Service)

(1) In order to create an environment in which the public may use digital signatures with a sense of safety and reliability and to exercise efficient control over licensed certification authorities, the Information Security Agency shall perform the functions set forth in the following subparagraphs:

1. In case of designating a licensed certification authority under Article 4, assistance with the examination of such facilities and equipment as the applicant for the designation shall prepare for meeting requirements for the said designation;
2. Assistance with the inspection of a licensed certification authority as provided in Article 14 (1);
3. Examination and technical assistance of protective measures as provided in Article 18-3;
4. Regular inspection as provided in Article 19 (2) as to whether facilities and equipment are securely operated;
5. Certification work, such as the issuance, control, etc. of authorized certificates for the licensed certification authorities;
6. Development of technology relating to digital signature certification, dissemination thereof, and research on standardization thereof;
7. Assistance with the promotion of international cooperation, including research on systems relating to digital signature certification and the reciprocal recognition thereof; and
8. Other necessary matters concerning digital signature certification control service.

(2) Articles 6, 7, 15 through 18, 18-2, 18-3, 19 (1), and 22 shall apply *mutatis mutandis* to the digital signature certification control service of the Information Security Agency. In this case, the "licensed certification authority" shall be deemed to be the "Information Security Agency" and the "subscriber" to be the "licensed certification authority". <*Amended by Act No. 7813, Dec. 30, 2005*>

(3) The Information Security Agency may levy charges, etc. for its performance of digital signature certification control service as referred to in paragraph (1), such as examination, technical assistance, inspection, issuance of authorized certificates.

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 25-2 (Obligation of Users)

The users shall take the following measures in order to verify whether or not a certified digital signature is true by referring to the particulars, etc. of the authorized certificate as set forth in Article 15 (2) 1 through 6:

1. A measure to ascertain whether the authorized certificate remains valid;
2. A measure to ascertain whether the authorized certificate has been suspended or revoked; and
3. A measure to ascertain such matters as set forth in Article 15 (2) 7 and 8.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 25-3 (Prohibition from Demand for Specific Authorized Certificate)

In verifying a digital signature by means of an authorized certificate, no person shall demand an authorized certificate issued only by a specific licensed certification authority without any justifiable reason therefor.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 26 (Compensation Responsibility)

(1) Where a licensed certification authority has caused damages to the subscribers or the users who have trusted its authorized certificates in connection with the performance of the certification work, it shall compensate such damages: *Provided*, That if the licensed certification authority proves that it has no fault, such compensation responsibility shall be exempted.

(2) A licensed certification authority shall subscribe for an insurance for compensating the damages under the provisions of paragraph (1).

[This Article Wholly Amended by Act No. 7813, Dec. 30, 2005]

CHAPTER V ADOPTION, ETC. OF DIGITAL SIGNATURE

CERTIFICATION POLICY

Article 26-2 (Formulation, etc. of Policies for Development of Digital Signature Certification System)

The Government shall formulate and carry out policies on matters set forth in the following subparagraphs in order to promote the development of digital signature and certification work, including the securing of the safety and reliability of digital signatures, promotion of wide and active use thereof, etc.:

1. Matters concerning a basic policy for the securing of safety and reliability of digital signature and the promotion of wide and active use thereof;
2. Matters concerning smooth cooperation among certification authorities in achieving the mutual recognition and common use of different certificates of digital signature and matters concerning technical standardization for such certificates;
3. Matters concerning the development of digital signature-related technique;
4. Matters concerning education and publicity designed for the promotion of wide and active use of digital signature;
5. Matters concerning improvement in systems and readjustment to the relevant Acts and subordinate statutes to promote wide use of digital signatures;
6. Matters concerning the provision of assistance and relevant information to organizations related to digital signatures;
7. Matters concerning the protection of rights and interests of subscribers and users that are related with certification work;
8. Matters concerning the reciprocal recognition of foreign digital signature and certificates as well as the promotion of international cooperation;
9. Matters concerning the promotion of digital signature-related industry and the training of manpower available for this industry;
10. Matters concerning protective measures to secure the safety of a licensed certification authority;
11. Matters concerning the adoption of pilot projects designed for the

promotion of wide and active use of digital signatures as well as matters concerning the survey of statistics and practical conditions in relation to the use of digital signature;

12. Matters concerning the use of encryption designed for the securing of safety and reliability of electronic messages; and
13. Such other matters as may be necessary for the securing of safety and reliability of digital signatures and for the promotion of use of digital signatures.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 26-3 (Cooperation among Certification Authorities in Achieving Mutual Recognition and Common Use of Different Certificates of Digital Signature)

(1) The Minister of Public Administration and Security shall carry out the matters set forth in the following subparagraphs in order to promote smooth cooperation among certification authorities in achieving the mutual recognition and common use of different certificates of digital signature: *<Amended by Act No. 8852, Feb. 29, 2008>*

1. Survey, research, and development on domestic and foreign standards for the mutual recognition and common use of different certificates of digital signature;
2. Establishment of standards related to the mutual recognition and common use of different certificates of digital signature and promotion of wide use thereof;
3. Adjustment to digital signatures and certification policy for the mutual recognition and common use of different certificates of digital signature; and
4. Other matters concerning the mutual recognition and common use of different certificates of digital signature.

(2) The Minister of Public Administration and Security may, if necessary, make the relevant agency or organization represent him for carrying out the matters set forth in subparagraphs of paragraph (1). In such cases, he/she may assist expenses required therefor as prescribed by Ordinance of the Ministry of Public Administration and Security. *<Amended by Act No. 8852, Feb. 29, 2008>*

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 26-4 (Development of Digital Signature-Related Techniques and

Manpower Training)

The Minister of Public Administration and Security shall carry out the matters set forth in the following subparagraphs for the purposes of technical development and specialized manpower training that are necessary for the promotion of the use of digital signatures: *<Amended by Act No. 8852, Feb. 29, 2008>*

1. Matters concerning research on digital signature-related technical level, technical study and development, and application thereof;
2. Matters concerning cooperation in and transfer of digital signature-related techniques;
3. Matters concerning the provision of information on digital signature-related techniques and the promotion of cooperation with agencies and organizations related thereto;
4. Matters concerning research on the supply and demand of manpower specialized in digital signatures and assistance for the specialized manpower training; and
5. Such other matters as may be necessary for the development of digital signature-related techniques and manpower training.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 26-5 (Implementation of Digital Signature-Related Pilot Projects)

(1) The Minister of Public Administration and Security may carry out pilot projects to promote the wide use of digital signatures as prescribed by Ordinance of the Ministry of Public Administration and Security. *<Amended by Act No. 8852, Feb. 29, 2008>*

(2) The Government may provide administrative, financial, and technical assistance in carrying out pilot projects as provided in paragraph (1).

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 26-6 (Assistance to Promote Use of Digital Signatures)

(1) The State or the local governments may provide financial assistance in promoting the wide use of digital signatures.

(2) In order to secure the safety and reliability of electronic commerce, the Government may formulate and carry out policies to reduce, or to give exemption from, fees, etc. payable for electronic commerce if authorized digital signatures are used in electronic transactions.

(3) Where a corporation or organization related with digital signatures carries out a project to encourage the use of digital signatures, the

Government may assist the whole or part of expenses required for the execution of the project concerned within the limits of budget.

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 26-7 (Deliberation Committee for Authorized Certification Policies)

(1) The deliberation committee for authorized certification policies (hereinafter referred to as the "deliberation committee") shall be established in the Ministry of Public Administration and Security in order to examine the matters of the following subparagraphs for the authorized certification policies: *<Amended by Act No. 8852, Feb. 29, 2008>*

1. Matters concerning a designation of the licensed certification authority under the provisions of Article 4 and for a cancellation of designation under the provisions of Article 12;
2. Matters concerning protection of the subscribers and users under the provisions of Article 27;
3. Matters concerning mutual recognition between the states under the provisions of Article 27-2;
4. Matters concerning major policies for settlement of disputes relating to the authorized certification work; and
5. Other matters deemed by the Minister of Public Administration and Security necessary in proceeding with the policies for certification of digital signature.

(2) The deliberation committee shall be consisted of less than 9 members including one chairperson, but one of the members shall be permanent.

(3) The members including the chairperson of the deliberation committee shall be appointed or commissioned by the Minister of Public Administration and Security as prescribed by Presidential Decree. *<Amended by Act No. 8852, Feb. 29, 2008>*

(4) The terms of members shall be three years, but they may be reappointed.

(5) Except for what are provided in this Act, the matters necessary for organization and operation, etc. of the deliberation committee shall be prescribed by the Presidential Decree.

[This Article Newly Inserted by Act No. 7813, Dec. 30, 2005]

CHAPTER VI SUPPLEMENTARY PROVISIONS

Article 27 (Protection of Subscribers and Users)

(1) The Government shall adopt such necessary measures as to deal with the complaints or damages of subscribers and users promptly and justly.

(2) Matters in detail concerning measures as provided in paragraph (1) shall be prescribed by Ordinance of the Ministry of Public Administration and Security. *<Amended by Act No. 8852, Feb. 29, 2008>*

[This Article Newly Inserted by Act No. 6585, Dec. 31, 2001]

Article 27-2 (Reciprocal Recognition)

(1) The Government may enter into an agreement with a foreign government on the reciprocal recognition of digital signatures.

(2) In case of the conclusion of the agreement under paragraph (1), it may form the basic contents of the agreement to grant a foreign certification authority or a certificate issued thereby the same legal status or effect as the licensed certification authority or the authorized certificate as provided in this Act. *<Amended by Act No. 6585, Dec. 31, 2001>*

(3) When an agreement on the reciprocal recognition of digital signatures has been concluded with a foreign government under paragraph (1), the Minister of Public Administration and Security shall give publicity to the contents of the agreement. *<Amended by Act No. 8852, Feb. 29, 2008>*

(4) If an agreement has been concluded with a foreign government under paragraph (1), a foreign digital signature or certificate shall be deemed to have the same legal effect as an authorized digital signature or an authorized certificate. *<Newly Inserted by Act No. 6585, Dec. 31, 2001>*

Article 28 (Imposition of Fees)

A licensed certification authority may impose necessary fees, such as service charges, on those who apply for the issuance of an authorized certificate or receive certification service. *<Amended by Act No. 6585, Dec. 31, 2001>*

Article 29 (Hearing)

The Minister of Public Administration and Security shall hold a hearing if he/she is to revoke a designation in accordance with Article 12 (1). *<Amended by Act No. 8852, Feb. 29, 2008>*

Article 30 (Delegation of Authority)

Part of the authority with which this Act vests the Minister of Public Administration and Security may be delegated to the head of a subordinate agency or entrusted to the President of the Korea Post as prescribed by Presidential Decree. *<Amended by Act No. 8852, Feb. 29, 2008>*

CHAPTER Ⅶ PENAL PROVISIONS

Article 31 (Penal Provisions)

Any person who falls under any of the following subparagraphs shall be punished by imprisonment for not more than three years or by a fine not exceeding 30 million won: *<Amended by Act No. 6585, Dec. 31, 2001>*

1. A person who holds a subscriber's digital signature creating key without any request on the part of the latter or who uses or discloses a subscriber's digital signature creating key without the consent of the latter, who has asked the former to hold the said key, in violation of Article 21 (3);
2. A person who uses by stealth or discloses another person's digital signature creating key in violation of Article 23 (1); and
3. A person who has an authorized certificate issued in the name of another person or aids such issuance, in violation of Article 23 (2).

Article 32 (Penal Provisions)

Any person who falls under any of the following subparagraphs shall be punished by imprisonment for not more than one year or by a fine not exceeding 10 million won: *<Amended by Act No. 7813, Dec. 30, 2005>*

1. A person who fails to retain the subscriber's certificates, etc. in violation of Article 22 (2);
2. Deleted; *<by Act No. 7813, Dec. 30, 2005>*
3. A person who uses an authorized certificate unlawfully by getting himself/herself out of the utilization scope or usage in violation of Article 23 (4); and
4. A person who transfers or rents an authorized certificate to other persons for the purpose of making them exercise it, or who receives a transfer or rent of the other persons' said certificate for the purpose of exercising it in violation of Article 23 (5).

[This Article Wholly Amended by Act No. 6585, Dec. 31, 2001]

Article 33 (Joint Penal Provisions)

If the representative of a juristic person, or an agent, an employee, or any other employed person of the juristic person or an individual has committed an offence under Article 31 or 32 with respect to the affairs of the juristic person or individual, not only shall such an offender be punished accordingly, but also the juristic person or individual shall be punished by a fine under

the relevant provisions: *Provided,* That this shall not apply in cases where the juristic person or individual has not neglected to give reasonable attention to and to supervise the relevant affairs to prevent such an offense.

[This Article Wholly Amended by Act No. 9208, Dec. 26, 2008]

Article 34 (Fine for Negligence)

(1) Any person who falls under any of the following subparagraphs shall be punished by a fine for negligence not exceeding 5 million won: *<Amended by Act No. 6585, Dec. 31, 2001; Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

1. A person who fails to report, or report the modification of, the rules of certification work in violation of Article 6 (1) or (3) (including cases of application *mutatis mutandis* as referred to in Article 25 (2)) or who fails to implement an order to modify the rules of certification work as provided in paragraph (4) of the same Article (including cases of application *mutatis mutandis* as referred to in Article 25 (2));
2. A person who refuses to provide certification services without any justifiable reason, or unjustly discriminates against subscribers or users, in violation of Article 7 (including cases of application *mutatis mutandis* as referred to in Article 25 (2));
3. A person who fails to make a report under Article 9 (1);
4. A person who fails to notify his/her subscribers of, or to report to the Minister of Public Administration and Security on, the cessation of certification work as provided in Article 10 (1) or the closure thereof as provided in paragraph (2) of the same Article;
5. A person who fails to transfer the subscriber's certificates, etc. to another licensed certification authority, or to report the impossibility of such a transfer, without any justifiable reason, in violation of Article 10 (3) or 12 (2);
6. A person who fails to submit the relevant documents and materials as referred to in Article 14 (1) or submits false records, or who refuses, obstructs, or evades an entrance and inspection by the relevant public officials;
7. A person who fails to give a notification as provided in Article 21 (4);

7-2. A person who fails to report on occurrence of obstacles to the information processing systems providing the certification work under the provisions of Article 22-3 (1);

8. A person who uses a similar mark that leads or may lead others to confuse an unauthorized certificate, etc. with an authorized certifi-

cate, or who falsely indicates the use of an authorized certificate, in violation of Article 23 (3);

9. A person who demands only the authorized certificate of a specific licensed certification authority in violation of Article 25-3; and

10. A person who fails to subscribe for an insurance in violation of Article 26 (2).

(2) The fine for negligence as referred to in paragraph (1) shall be imposed and collected by the Minister of Public Administration and Security as prescribed by Presidential Decree. *<Amended by Act No. 8852, Feb. 29, 2008>*

(3) Any person who is dissatisfied with a disposition of fine for negligence as referred to in paragraph (2) may raise an objection to the Minister of Public Administration and Security within 30 days after he/she was notified of such a disposition. *<Amended by Act No. 8852, Feb. 29, 2008>*

(4) When a person, who is subject to a disposition of fine for negligence as referred to in paragraph (2), raises an objection under paragraph (3), the Minister of Public Administration and Security shall, without delay, notify the competent court thereof, and the court so notified shall, in turn, proceed to a trial on fine for negligence in accordance with the Non-Contentious Case Litigation Procedure Act. *<Amended by Act No. 7813, Dec. 30, 2005; Act No. 8852, Feb. 29, 2008>*

(5) When an objection is not raised within such period as prescribed in paragraph (3) nor is a fine for negligence paid, the fine for negligence shall be collected by referring to the practices of dispositions on default of national taxes.

ADDENDUM

This Act shall enter into force on July 1, 1999.

ADDENDA *<Act No. 6360, Jan. 16, 2001>*

Article 1 (Enforcement Date)

This Act shall enter into force on July 1, 2001.

Articles 2 through 6 Omitted.

ADDENDA *<Act No. 6585, Dec. 31, 2001>*

Article 1 (Enforcement Date)

This Act shall enter into force on April 1, 2002.

Article 2 (Transitional Measures concerning Liability)

The previous provisions shall apply to liability for any damage that was caused by a licensed certification authority in the process of performing its certification work before the enforcement of this Act.

Article 3 (Transitional Measures concerning Application of Penal Provisions)

The previous provisions shall prevail in the application of penal provisions to an offence that was committed before the enforcement of this Act.

Article 4 Omitted.

ADDENDA *<Act No. 7428, Mar. 31, 2005>*

Article 1 (Enforcement Date)

This Act shall enter into force one year after the date of its promulgation.

Articles 2 through 6 Omitted.

ADDENDA *<Act No. 7813, Dec. 30, 2005>*

(1) (Enforcement Date) This Act shall enter into force six months after the date of its promulgation: *Provided*, That the amended provisions of Article 4 (4) of the Act shall enter into force on the date of its promulgation.

(2) (Transitional Measures concerning Application of Penal Provisions) The previous provisions shall govern any application of penal provisions against the acts taken before the enforcement of this Act.

ADDENDA *<Act No. 8852, Feb. 29, 2008>*

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation. (Proviso Omitted.)

Articles 2 through 7 Omitted.

ADDENDUM *<Act No. 9208, Dec. 26, 2008>*

This Act shall enter into force on the date of its promulgation.