[Interim Translation (official: Japanese)]
Public Notice No. 2
Ministry of Internal Affairs and Communications
Ministry of Justice
Ministry of Economy, Trade, and Industry

In order to implement the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000) and Implementation Ordinance on the Act on Electronic Signatures and Certification Business (Ordinance No. 2 of Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade, and Industry of 2001), guidelines on accreditation of specified certification business under the Act on Electronic Signatures and Certification Business have been defined and published as follows.

April 24, 2009

Guidelines on Accreditation of Specified Certification Business based on the Act on Electronic Signatures and Certification Business

Article 1 (Purpose)
The purpose of this Guidelines is to facilitate the enforcement of the Act on Electronic Signatures and Certification Business (hereinafter called the "Act") by means of defining details on accreditation criteria regulated under the provisions of paragraph 3, Article 2, and paragraph 1, Article 6 (including cases in compliance with paragraph 2, Article 7 (including cases where it is applied mutatis mutandis pursuant to paragraph 2, Article 15), paragraph 3, Article 9 (including cases where it is applied mutatis mutandis pursuant to paragraph 2, Article 15), and Articles 2 and 4 of the Implementation Ordinance on Electronic Signatures and Certification Business (hereinafter called the " Ordinance").

Article 2 (Definitions)
Terms employed in the Guidelines herein shall be based on terms employed in the Act and the Ordinance.

Article 3 (Criteria on Electronic Signature in pertaining to Specified Certification Business)

The electronic signature system that satisfies the criteria set forth in Article 2 of the Ordinance shall be any of the following:

(i) RSA/SHA-1 (object identification 1 2 840 113549 1 1 5) , RSA/SHA-256 (object identifier 1 2 840 113549 1 1 11), RSA/SHA-384 (object identifier 1 2 840 113549 1 1 12) or RSA/SHA-512 (object identifier 1 2 840 113549 1 1 13) with modulus consisting composite numbers of more than 1,024 bits.

(ⅱ)RSA-PSS(object identifier 1 2 840 113549 1 1 10)/SHA-1(object identifier 1 3 14 3 2 26), RSA-PSS(object identifier 1 2 840 113549 1 1 10)/SHA-256(object identifier 2 16 840 1 101 3 4 2 1), RSA-PSS(object identifier 1 2 840 113549 1 1 10)/SHA-384(object identifier 2 16 840 1 101 3 4 2 2) or RSA-PSS (object identifier 1 2 840 113549 1 1 10)/SHA-512(object identifier 2 16 840 1 101 3 4 2) with modulus consisting composite numbers of more than 1,024 bits.

(iii) ECDSA /SHA-1 (object identification 1 2 840 10045 4 1), ECDSA/SHA-256(object identifier 1 2 840 10045 4 3 2), ECDSA/SHA-384 (object identifier 1 2 840 10045 4 3 3) or ECDSA/SHA-512(object identifier 1 2 840 10045 4 3 4) with elliptic curve definition and order consisting of more than 160 bits.

(iv) DSA/SHA-1 system (object identification 1 2 840 10040 4 3) with modulus consisting of elements of 1,024 bits.

Article 4 (Measures Necessary for Access Control to Certification Facility Room)

Measures necessary for access control corresponding to the level of importance of operation as provided in item (i), Article 4, of the Ordinance are classified as follows and shall meet requirements specified in the corresponding items

(i) Certification facility room (room where facilities for certification business are installed, excluding room where facility employed in certification business which is used chiefly for registration of electronic certificate users (hereinafter called the "registration terminal") and hereinafter the same) shall satisfy the following requirements

(a) Access to be authorized only with identification of distinctive physical characteristics (referring to cross-check with pre-registered fingerprint, iris, or other distinctive physical characteristics of private individuals) of two or more persons entering the room.

(b) Control over the number of persons entering the room and identical number of persons leaving the room.

(c) Alarm to be set off in case abnormal time is spent on operation of access control devices.

(d) Remote surveillance devices and video recording devices to be installed for

monitoring automatically and continuously persons entering and/or leaving the room and persons inside the room.

(ii) Measures such as locking to be executed to prevent easy access of registration terminal by unauthorized personnel in room where registration terminal is installed and which is not certification facility room.

Article 5 (Measures Necessary to Prevent Unauthorized Access, etc., to Certification Business Facilities) Measures necessary to prevent unauthorized access, etc., by means of telecommunications circuits as provided in item (ii), Article 5, of the Ordinance are to be the following:

(i) In connection of certification business facilities via telecommunications circuit, certification business facility (excluding registration terminal) shall be equipped with firewall and system to detect unauthorized access, etc., in order to prevent unauthorized access.

(ii) If certification business facilities are separated into two or more components, measures are to be taken to prevent erroneous recognition of facility transmitting message and eavesdropping or tampering with the communication from one component to another component.

(iii) If computer systems used for receiving user signature verification codes, user information, and user identification codes through telecommunications lines are installed, measures are to be taken to prevent erroneous recognition of a computer used for sending this information, as well as the eavesdropping on or tampering with the communications content from a computer to the certification business facility.

Article 6 (Measures To Prevent Operation of Certification Business Facilities by Persons Without Authorization)

(1) Measures to prevent operation of certification business facilities by persons without authorization are to satisfy the following requirements.

(i) Authority for operation of certification business facilities to be defined for each operator.

(ii) When operating a certification business facility automatically using user information/user identification codes, it should be possible to set user identification codes, install the computer systems (in rooms that can be locked) that are to be used to receive user signature verification codes, user information, and user identification codes via telecommunication lines. It also should be possible to set the functions for identifying the user information/user

identification codes sent from a computer system via telecommunication lines, and to confirm user information/user identification codes.

(iii) Facilities to be set to make remote operation via telecommunications circuit impossible. However, this shall not apply to operation of registration terminal necessary for electronic certificate management, such as electronic certificate issue or invalidation requests.

(iv) The location of certification business facilities is not to be displayed.

(2) The functions for recording operations of certification business facilities prescribed in item (iii), Article 4, of the Ordinance are as follows:

(i) Function for recording name of requesting person, content, date, result, etc., of each operation as operation history.

(ii)Function for displaying operation history for specific operator.

Article 7 (Measures Necessary To Prevent Damages on Certification Business Facilities, etc., from Natural Disasters) Measures necessary to boost resistance to damages from disasters such as power failure, earthquake, and flood, prescribed in item (v), Article 5, of the Regulations are classified as follows and shall meet requirements specified in the corresponding items.

(i) Certification business facilities: Fixture of system components and other earthquake-resistant measures to be implemented to prevent falling or displacement of facility components from earthquake of foreseeable magnitude.

(ii) Certification facility room: The following requirements are to be satisfied.

(a) Measures to be taken to prevent flooding.

(b) Partitioning by walls

(c) Installation of automatic fire detectors and fire extinguishers.

(d) Installation in fire-protection areas.

(e) Measures to be taken against power failure for power source facilities used inside the room.

(iii) Structure in which the certification facility room is to be installed, the following requirements are to be satisfied.

(a) Foundation of land on which the structure is to be built is to have little possibility of earthquake damages. This shall not apply, however, in unavoidable cases and when measures are to be taken to prevent unequal subsidence.

(b) Structure to satisfy the provisions of the Construction Standards Act (No. 201 of 1950) for safety against earthquakes and relevant orders and ordinances.

(c) Structure to be fire-resistant or quasi-fire-resistant as provided in the Construction Standards Act.

Article 8 (Items for Explanation to Prospective Users)

Items to be explained to prospective users prescribed in item (i), Article 6 of the Ordinance are to contain the following items:

(i) In designated certification business, persons who allow false certification to users by means of false user application are to be penalized under provision of Article 41 of the Act.

(ii) In order to acquire legal effect corresponding to handwritten signature and seal impression, user signature code for electronic signature is to be managed with adequate caution.

(iii) In case user signature code is endangered (namely, placed in a state of being available to other persons through theft, leakage, etc.; hereafter the same) or is likely to be endangered, in case of change in provisions recorded in the electronic certificate, or in case use of the certificate is discontinued, request for invalidation of the said certificate must be made promptly.

(iv) Algorithm employed for electronic signature in use of electronic certificate for designated certification business must be that designated by the certification business provider.

Article 9 (Items To Be Shown in User Application, etc.)

User application and other written or application-related information in item (ii), Article 6, of the

Ordinance shall show or contain in recording the following items:

(i) The name, address, and date of birth of the applicant

(ii) Specific uses of the electronic certificate for which application was submitted.

(iii) Name of applicant shown in alphanumerical characters.

(iv) Handwritten signature of the applicant or seal impression of seal for the certification, if official seal registration certificate is to be employed as method of confirming identity of the user (excluding cases in which information on application is to be transmitted).

(v) In application by proxy, the name and handwritten signature of the proxy applicant in addition to the aforementioned items, seal impression from the seal (if official seal registration certification is to be employed as method of confirming the identity of the proxy), and reason for application by proxy.

Article 10 (Measures To Prevent Erroneous Recognition between Accredited Certification Business and Other Business) Appropriate measures to prevent erroneous recognition between accredited certification business and other business by the user or others prescribed in item (vii), Article 6, of the Ordinance shall include the measures listed below.

(i) Do not use for business other the accredited certification business, except for the following:

(a) Use for mutual certification with certification business provided by national or local governments in compliance with standards comparable or exceeding other accredited certification business.

(b) Use when necessary to maintenance or management of the accredited certification business.

(ii) Accredited certification business shall be specified according to the value for the electronic certificate relating to the issuer signature verification code that has been transformed by one or more of SHA-1, SHA-256, SHA-384 or SHA-512.

Article 11 (Providing Information to Signature Verifying Party)

Information necessary as provided in item (ix), Article 6, of the Ordinance shall contain the items described as follows:

(i) The party verifying signature shall confirm the issuer of the electronic certificate by obtaining the issuer signature verification code and verifying the electronic signature by the issuer in the electronic certificate.

(ii) The signature verifier shall confirm the objective of electronic certificate use, range of use of the certificate, and its range of authority (including requirements for use reported in advance to the user).

(iii) The signature verifier is to confirm through appropriate means that information on invalidation of the electronic certificate is not recorded.

Article 12 (Regulations on Execution of Certification Business)

(1) Regulations on execution of certification business as provided in item (xiii) Article 6, of the Ordinance shall contain provisions shown in the following items:

(i) Name and contact address of the certification business provider (address, telephone number, facsimile number, and electronic mail address)

(ii) Restriction items when restrictions apply to objective, target, and range of certificate use.

(iii) Restriction items if restrictions apply to range of guarantee and responsibility to be taken by the accredited business.
(iv) Items on methods of confirming the identity of the user and method of user application
(v) Items on requesting invalidation of electronic certificate
(vi) Items on method of confirming information on invalidation of electronic certificate and period for confirmation
(vii) Items on security in certification business (including items on handling private information on the user)
(viii) Items on charges related to use of certification business
(ix) Items on preservation of books and documents
(x) Items on abolition of business
(xi) Acts and regulations applied in case of dispute between accredited businesses and items on procedure for resolution
(xii) Items on revision of relevant regulations and items on method of informing users and other persons

(2) Provisions listed in item (x) in the preceding paragraph shall also apply to report to users for abolition of certification-related operations 60 days prior to abolition (on the date of expiration of certification business if certification business extension is not executed) (although not applicable under unavoidable circumstances such as invalidation of accreditation under paragraph 1, Article 14 of the Act) and for invalidation procedure for electronic certificate issued to user by date of abolition of certification business.

Article 13 (Permission, etc., relating to the Operation, etc., of Facilities used for Certification Business) Permission for access to room where certification business facilities are installed and operation of such facilities under Item (xvi), Article 6, of the Ordinance and appropriate management of the identification code related to such permits shall be implemented by satisfying the following requirements.

(i) Access to the certification facility room is to be executed in multiple number of persons only.
(ii) If a person not authorized for access should be required to access the certification facility room for facility maintenance and other circumstances necessary for business management, a multiple number of persons with authority shall escort the said person.
(iii) Identification code for the system manager shall be placed under exceptionally strict control.

Article 14 (Measures Necessary to Prevent Leakage of Issuer Signature Code)
Measures necessary to prevent leakage of issuer signature code provided in item (xvii), Article 6 of the Ordinance shall satisfy the following requirements:
(i) Generation and management of issuer signature code shall be executed by a multiple number of persons in the certification facility room with computer system specified for this purpose under item 4, Article 4 of the Ordinance.
(ii) Duplication of the issuer signature code needed for backup shall be executed in any of the following methods.

(a) Execution by computer system specified for this purpose under item 4, Article 4 of the Ordinance and issuer signature code duplicated for backup to be stored in a location with security comparable to that of the certification facility room.
(b) information on the issuer signature code shall be split in the certification facility room and stored separately in separate secure locations by separate persons (when a number of persons are to assemble when issuer signature code is to be restored).

(iii) Modification in certification business facilities to enable or disable use of issuer signature code shall be executed by a multiple number of persons inside the certification facility room.
(iv) If use of the issuer signature code is to be terminated, it and the duplicated issuer signature code shall be disposed of simultaneously completely by a multiple number of persons through physical destruction or complete initialization.

Supplementary Provision
This Guidelines shall come into force as from April 1, 2001.

Supplementary Provision(Public Notice No.13 of Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade, and Industry)
1. This Guidelines shall come into force as from the date of promulgation.
2. When this notice come into force, for persons accredited set forth in paragraph 1, Article 4 of the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000, hereinafter referred to as the “Act”), in applying the each of the following provisions, with regard to the application of the term prescribed in each of the item from the date in which this notice come into force, the provisions then in force shall remain applicable.

(i) Item (i), Article 3 of the Guidelines on Accreditation of Specified Certification Business based on the Act on Electronic Signatures and Certification Business after it has been revised: one year
(ii) Item (ii), Article 10 of the New Guidelines, the term until receiving renewal of accreditation set forth in paragraph 1, Article 7 of the Act

Supplementary Provision (Public Notice No. 9 of Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade, and Industry)
This Guidelines shall come into force from the date of promulgation.

Supplementary Provision (Public Notice No. 11 of Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade, and Industry)
This Guidelines shall come into force from the date of promulgation.