[Interim Translation (official: Japanese)]
April 2, 2001
Information and Communications Policy Bureau, Ministry of Internal Affairs and Communications
Civil Affairs Bureau, Ministry of Justice
Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry

The Policies of Investigations of Designated Investigative Organizations based on the Act on Electronic Signatures and Certification Business

Section 1. Objective

1. Objective

The Policies are to facilitate the operation of the Electronic Signatures and Certification Business system by means of identifying the policies of investigations conducted by the Designated Investigative Organizations pursuant to the Act on Electronic Signatures and Certification Business.

2. Definitions

For the purpose of these Policies, the "Act" refers to the "Act on Electronic Signatures and Certification Business (Act No. 102 of 2000)", the "Ordinance" refers to the "Implementation Ordinance on Electronic Signatures and Certification Business (Ordinance No. 2 of the Ministry of Internal Affairs and Communications, the Ministry of Justice, and the Ministry of Economy, Trade and Industry, 2001).",, the "Guidelines" refers to the "Guidelines on Accreditation of Designated Certification Business based on the Act on Electronic Signatures and Certification Business."

Section 2. Matters related to the facilities provided for the use of certification business

1. General

Conforming with the criteria for the facilities used for certification business set forth in item (i), Paragraph 1, Article 6 of the Act, Article 4 of the Ordinance, and Articles 4 through 7 of the Guidelines means that not only facilities that satisfy the criteria are established in light of the technical standards and other specifications in force at the time of the qualification, but also Specified Certification Business that can be conducted properly, smoothly and safely and where such measures are taken to fulfill that purpose.

2. Matters relating to encryption devices

(1) "Exclusive electronic computer" (hereinafter referred to as the "encryption devices") set forth in paragraph 4, Article 4 of the Ordinance means devices equipped with the functions specified below for minimizing the occurrence of events such as leakage, damage, loss, and other trouble with the issuer signature codes to the greatest extent possible.

(i) If there is an interface for input and output using an encryption device concerning unprotected important data such as unencrypted codes and certification data etc., such interface shall be physically independent from the interfaces for inputting and outputting other data.

(ii) The encryption devices shall have the functions specified below, and whether there is authority or not for each function shall be specified for each operator of the encryption devices.

(a) Operator functions: Functions for implementing usual encryption functions such as encryptions and signatures.

(b) Administrator functions: Functions for managing the encryption devices, such as initializing the encryption devices themselves and entering signature codes and other important parameters.

(iii) To avoid data theft such as issuer signature codes, the encryption devices shall take one of the physical security measures specified below:

(a) If the encryption device consists of a single IC chip, the IC chip shall be covered with an opaque coating made of a rigid, hard-to-remove material;

(b) If the encryption device is covered, tamper-proofing measures shall be taken to avoid physical intrusions by means such as disabling the functions of the encryption devices and invalidating the internal data; or

(c) If the cabinet of the encryption devices has an exhaust slit or an air vent, such slit or vent shall be small enough and measures shall be taken to prevent the inside of the cabinet from being probed without being detected.

(iv) With respect to the management of the issuer signature codes relating to the encryption devices, the following measures shall be taken:

(a) If the issuer signature codes are to be generated inside the encryption devices, secure algorithm for generating pseudo-random numbers is to be used.

(b) If the issuer signature codes are to be input or output into the encryption devices, such input and output shall be performed directly with the encryption devices and shall be in either of the following methods:

1) The issuer signature codes shall be encrypted before being input or output; or

2) The issuer signature codes shall be divided into two or more constituents, then be input or output. In this case, a certification shall be performed on the operator in charge of each constituent of the issuer signature codes. Each constituent of the issuer signature codes shall be divided and recombined in the encryption devices.

(c) If the issuer signature codes are to be stored in the encryption devices unencrypted, the measure shall be taken to make the mechanism to ensure that no one can access from the outside

(d) If the issuer signature codes are to be discarded, the system initiating such a function shall be able to invalidate the issuer signature codes as unencrypted as well as invalidate other security parameters.

(2) Notwithstanding Paragraph (1) above, if the operating system etc. or other software on the computer incorporating the encryption devices satisfies the functions and requirements specified below, and if equivalent security can be achieved by taking security measures for the entire certification business facilities and the entire certification facility room, such measures may replace the above set of measures.

(i) All software for driving the encryption devices shall have been installed only in the form of executable code.

(ii) The encryption software, signature codes and other important security parameters, control information, status information and other information shall be under the control of the operating system equipped with functions for checking inputs and outputs.

(iii) The system shall use an operating system equipped with functions for protecting the signature codes, certification data, and other important security parameters, along with other information, from unauthorized access and other wrongful attempts.

(iv) If the system does not satisfy the requirements for having a physically independent interface specified in item (i) (a) above, the input and output of important data shall be conducted by a secure method in order to prevent any confusion with other data where using the operating system for the computer equipped with the encryption devices.

(v) If the system is unable to identify the authority of each operator in the case of item (i) (b) above, measures shall be taken to allow for the identification of the operator by using the operating system or other facilities on the computer equipped with the encryption devices.

(vi) If the encryption devices are tamper-proofed by any of the measures specified below, it shall be protected by storing the non-operating device in a safe place, by monitoring

the status against physical attacks on the computer by means of monitoring equipment, and by using the operating system or other facilities on the computer against logical attacks.

(a) The IC chip shall be covered with an opaque coating capable of detecting attempts of unauthorized access or other wrongful conduct.

(b) The encryption devices shall be covered or otherwise handled with an opaque cabinet and shall be covered with an opaque coating capable of detecting attempts of unauthorized access or other wrongful conduct.

(vii) With respect to item (1) (iv) (b) above, measures shall be taken to disable inputs and outputs by a measure other than those specified in items (1) (iv) (b) 1) and 2) by means of the operating system or other facility on the computer equipped with the encryption device.

Section 3. Matters relating to the methods for confirming the identity of the Users of the Certification Business

1. General

The accredited certification business operator shall be able to identify in advance the methods adopted in its own business, from among the methods of confirming the identity of users set forth in Article 5 of the Ordinance, and the category of the documents for confirming the identity of users by using such methods.

2. Procedure for confirming the identity of users

(1) In confirming the identity of a user, one shall confirm the authenticity of the document for confirming the identity of the user, in terms of the entries, format, expiry date, etc.

(2) A letter of proxy which is required to be submitted in a case where the application for use is done by proxy means a document that clearly indicates the details of the application for use which the user authorizes the proxy to file (the said details shall conform to the entries in the application for use).

(3) If verifying the authenticity of the user will not occur simultaneously with receiving the user signature verification codes from the user, one shall check that the person who files the user signature verification codes corresponds to the verifying applicant.

(4) If verifying the authenticity of the user at the time of the renewal of the electronic certificate pursuant to the provisions of paragraph 2, Article 5 of the Ordinance, one shall verify the electronic signature given by the user with the information on the application for use and shall check that the information on the invalidity of the

electronic certificate related to the electronic signature.
(5) In the case of any discrepancy when confirming the identity of the user, the user shall be required to follow procedures to confirm the user in accordance with the procedures set forth in specified documentation in advance.

Section 4. Matters relating to the methods of conducting the Certification Business (except for the method for confirming the identity of the user)
1. General
Conforming with the criteria for the methods of the certification business set forth in item (iii), Paragraph 1, Article 6 of the Act, Article 6 of the Ordinance, and Articles 8 through 14 of the Guidelines means that the methods satisfy the criteria on a level high enough to conduct the certification services appropriately, smoothly and safely in light of the technical standards and other specifications in force at the time of the qualification, and where the documents and other information that set forth the procedures and other details for the certification services clearly stipulate that operations must be conducted with methods to satisfy the standards, and where such requirements are understood, implemented and maintained by all employees according to their roles.

2. Compilation and other handling of the user signature codes by an accredited certification business operator
(1) The compilation of the user's signature codes "in the event the certification business operator compiles the user's signature codes" as set forth in paragraph 3, Article 6 of the Ordinance shall be conducted by one or more person in a certification facility room or in an environment where similar safety is ensured.
(i) The user signature code is to be generated by multiple persons in the certification business facility room or in an environment in which comparable safety has been secured.
(ii) Handling of user signature code, including transfer and output, is to be executed in an environment in which security equivalent to that when the said code was generated.
(iii) When the said user signature code is issued or sent to a specific user, receipt of the user identification code must be verified with a receipt or comparable document.
(2) "In case the user signature code is generated by the certification business and if using the method of the certification business receiving the user signature verification code corresponding to the relevant user signature code via telecommunications" as provided in the Order, Article 6, item 3-2, it is to include the following measures.

(i) The user identification code used to identify such a user must be created using secure algorithm for generating pseudo-random numbers in a certification business facility room or in an environment in which comparable safety has been secured, and the process must be involved by multiple number of persons.
(ii) When electronic certificates are issued to a specific user, receipt of the user identification code must be verified.
(iii) The user identification code is to be stored by encrypting or implemented other measures in a certification business facility room or in an environment in which comparable safety has been secured.
(iv) When a user sends a user identification code, measures must be implemented to prevent erroneous reception of the said code by the computer system, as well as the wiretapping and tampering of the said code.
(v) Measures must be implemented immediately to prevent use of the user identification code employed in identifying the user for subsequent identification processing.

3. Confirming that the user holds a user's signature code The user's signature verification codes recorded in electronic certificates set forth in (d) in item (v), Article 6 of the Ordinance, confirming that the user holds the user's signature codes corresponding to the user signature verification codes is performed by verifying an electronic signature made by means of the user's signature codes with the user's signature verification codes or otherwise.

4. Verification of the user's attributes, etc.
The entry into the electronic certificate of the referent of information that records that a certificate of the user's managerial position or other details recorded in the electronic certificate is out of the scope of accreditation by Act, shall correspond to the "appropriate measures to prevent misunderstanding the certification of the user's managerial position and other attributes related to the accredited certification services." as set forth in item(viii), Article 6 of the Ordinance.

5. Methods for providing the issuer signature verification codes, etc.
The recording of the referent of the issuer signature verification codes and other necessary information in the electronic certificate shall correspond to "measures to have easy access to the issuer signature verification codes and other necessary information" as set forth in item (ix), Article 6 of the Ordinance.

6. Procedure for the invalidation of electronic certificate

(1) If the certification business operator has followed the procedures for invalidation of an electronic certificate, the operator shall without delay take all measures set forth in item 11, Article 6 of the Ordinance.

(2) "to be able to easily verify information on the invalidation", set forth in the same item means taking measures for disclosing a list of invalid electronic certificates that has recorded the electronic certificates with invalidation records, providing information about the status of the electronic certificate (whether records and other details of invalidation are recorded or not) by means of a protocol for checking the status of the electronic certificate online, and other measures having equivalent functions.

7. Disclosure of documents, etc. used to confirm the identity of the user

When the documents and other information used to confirm the identity of the user are disclosed in accordance with the provisions of item (xiv), Article 6 of the Ordinance, one shall check that the applicant for the disclosure is the holder of the electronic certificate issued based on the application documents.

8. Matters related to the provisions of the operation procedure, etc.

(1) "Matters on the auditing of business" set forth in (d), in item (xv), Article 6 of the Ordinance means the criteria for auditing the confirmation that the certification businesses are conducted appropriately in accordance with the provisions set forth in item (xiii), Article 6 of the Ordinance and the operation procedures and other details provided for in the provisions of (a) in the same item, and shall make sure that the facilities, provisions and other details are appropriately reviewed according to the results of the audit and the recent trends in security solution technology.

(2) "Measures required to prohibit the use of the accessed information for purposes other than those intended when confirming the identity of the user" set forth in (f) in the same item are as follows:

i) Provisions are clearly set forth for handling and protecting personal information that clarifies the handling of the information.

ii) Obtaining the approval of the user regarding the method of handling the information and the scope of entries in the electronic certificate.

(3) "Matters on risk management" set forth in (g) in the same item means a set of solutions and recovery procedures for the endangerment of the issuer signature codes and the occurrence of any disorder due to a disaster or other incident, and shall include

the following:

(i) If the issuer signature codes are compromised or likely to be compromised, the invalidation procedure shall be immediately followed for all issued electronic certificates.

(ii) The notification of the compromise of the issuer signature codes or the occurrence of a disturbance due to a disaster or other incident, and the disclosure of such facts to the signature verifier and the method thereof.

(iii) If the issuer signature codes are compromised or likely to be compromised, or if the provision of information on the invalidation of the electronic certificate for the signature verifier due to a disaster or a breakdown of the certification businesse facilities has suspended for a time exceeding the time set forth in the provisions on the implementation of the certification services set forth in item (xiii), Article 6 of the Ordinance, and if such suspension has not been disclosed to the verifier, the confirmed matters such as the nature of the disorder, the date of the incident, and the measure status shall be immediately notified to the competent minister.

9. Measures for specifying accredited certification business

"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" provided for in the Guidelines, Article 10, item 2, refer to measures in which the user or other parties are able to specify the accredited certification business by employing values obtained by converting the electronic certificate value recorded in the issuer signature verification code corresponding to the issuer signature code used by the accredited certification business with one or more of the hash values SHA-1, SHA-256, SHA-384 or SHA-512 and at the same time include execution of tampering-prevention measure and disclosure.

Section 5. Matters relating to the provisions for the implementation of Certification Business

(1) The provisions for the implementation of certification services set forth in item (xiii), Article 6 of the Ordinance shall stipulate not only the matters listed in Article 12 of the Guidelines, but also the format of the electronic certificate, standards for recording thereof, languages used for such recording, and items relating to the matters to be

recorded and the details thereof.
(2) "Items on requesting the invalidation of electronic certificate" listed in item (v), Paragraph 1, Article 12 of the Guidelines shall include the reasons for the invalidation of the electronic certificate (including those stemming from an act of the certification business operator), the method of requesting invalidation, matters to be specified or recorded in the invalidation request or request for information, the method of confirming the identity of the claimant, the procedure for recording invalidation information, and the cycle of processing the operations related to the invalidation.
(3) " Items on method of confirming information on invalidation of electronic certificate and period for confirmation" set forth in item (vi), paragraph 1, Article 12 of the Guidelines shall include the nature of the information to be disclosed concerning the invalidation, the method of disclosing such information, the cycle of renewal of an electronic certificates invalidation list, the method of notifying the user of the electronic certificate of the invalidation, the method of proceeding with an inquiry received concerning the information of invalidation of the electronic certificate from the signature verifier after the expiration of the specified period.
(4) "Items on security in certification business (including items on handling private information on the user)" provided for in the Guidelines, Article 12, paragraph 1, item 7, must include items related to security standards, technical standards, etc., employed by such a certification business.

Section 6. Matters relating to the Preservation of Books, etc.
1. General
(1) Of all books and documents listed in each item of paragraph 1, Article 12 of the Ordinance, the application for use or a request form for the invalidation of an electronic certificate, or other documents to be filed or information to be sent by the user shall contain the date and time of the receipt and the information concerning the identification of the receiving person as related to one another.
(2) Of all the items in the same paragraph, records related to the preparation of electronic certificates and records related to the implementation of other certification services shall contain the dates and times of such implementations, and the information concerning the identification of the persons who conducted such services, and the identifications of the persons responsible for such services as related to one another.

2. Books and documents relating to the application for use in Certification Business
(1) " Records on compilation and management of issuer signature codes" set forth in (h)

in item (i), paragraph 1, Article 12 of the Ordinance means the dates and times of implementations of item (2), Paragraph 1 above, and information concerning the identification of the persons who conducted such services and the persons responsible for such services, and records required for a person designated by the Japanese government pursuant to paragraph 1, Article 17 of the Act to investigate if the compilation and management of the issuer signature codes are conducted in accordance with the Act, Ordinance, and Guidelines at the time of renewal of the accreditation, and shall pertain to the following:

(i) Specification of the scope of use of the issuer signature codes;

(iii) Compilation and storage of the issuer signature codes;

(iv) Reconfiguration of the certification service facilities that enables or disables the use of the issuer signature codes;

(v) Generation of a backup copy of the issuer signature codes;

(vi) Restoration of the issuer signature codes; or

(vii) Discarding of the issuer signature codes.

(2) "Receipts from the user" set forth in (i) in item (i), paragraph 1, Article 12 of the Ordinance means receipts with an on-paper signature or electronic signature made by the user.

3. Books and documents relating to the invalidation of electronic certificates

"Records on the evaluation for invalidation" set forth in (a) in item (ii), paragraph 1, Article 12 of the Ordinance means records including documents used to confirm the identity of the claimant of the invalidation of an electronic certificate.

4. Matters related to Books and Documents on the structural management of the certification business operator

(1) Records specified in (c) in item (iii), paragraph 1, Article 12 of the Ordinance means records including a structural chart or system diagram concerning the personnel engaged in the certification business.

(2) Records relating to (e) in the same item menas audit records (including audits to be conducted irregularly), audit reports (those concerning regular audits), and corrective action reports based on the audit findings.

5. Matters relating to Books and Documents on Facilities and Safety Measures

(1) Records set forth in (a) in item (iv), paragraph 1, Article 12 of the Ordinance means records including the dates and times and venues of in and out of the rooms,

information about the identification of personnel entering and leaving, records of operation of devices in relation to such entering and leaving, and records of alarms emitted.
(2) Records set forth in (b) of the same item means abnormality records (such as the dates and times of abnormalities, IP addresses of the source computers, IP addresses of the destination computers, and communications protocols used) from the history of the firewalls and intrusion detection systems.
(3) Records set forth in (c) of the same item means records related to the operation of certification service facilities which are records of operations other than those related to ordinary tasks and those related to disturbances.
(4) Records set forth in (d) of the same item means rules concerning the management of licenses prepared for each form of license and records of the performance of authority management in accordance with those rules.
(5) Records set forth in (e) of the same item means records of facility maintenance and those including the history of system modifications.
(6) Records set forth in (f) of the same item means records concerning unauthorized access to the certification facility room, suspension of the certification service facilities, or wrongful operation thereof, and the suspension or wronful operation of the controller of in an out of the certification facility room (except for the records included in the history of the firewalls and intrusion detection systems which indicate abnormal states), reports concerning such disorders, and those including reports of the recoveries therefrom.

6. Electromagnetic recording
Preservation on "recording media related to recording by electromagnetic means" set forth in paragraph 4, Article 12 of the Ordinance means preservation with a method that satisfies either of the following requirements:
(i) Computers and other equipment, operating systems, and applications should be maintained and stored to make it possible to display the details of such recording media. If a computer or other equipment, operating system, or application is upgraded, one should ensure compatibility with the recording media, thus preventing display failures.
(ii) If any difficulty in using the recording media is expected, one may store a copy of the details in a different recording media. At that time, however, enough care shall be exercised to prevent the integrity and confidentiality of the stored details from being compromised.