Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
1 Criteria for the facilities		**1.1 Measures Necessary for Access Control to Certification Facility Room**	
1111	Of the facilities provided for use of the business pertaining to the application, the electronic computers used for compiling or managing electronic certificates (magnetic recordings compiled to certify that the particulars (hereinafter referred to as the “user signature verification code”) used to verify that the user is the person who performed electronic signature are related to the concerned user and other facilities (hereinafter referred to as the “certification business facilities”) shall be set up at locations devised with the required measures in accordance with the importance of business for managing entrance and departure from the site. (Article 4)	Measures necessary for access control corresponding to the level of importance of operation as provided in item 1 of Article 4 of the Ordinances are classified as follows and shall meet requirements specified in the corresponding items (i) The "certification facility room" is described as the room in which the certification business facilities (as defined in item 1 of Article 4 of the Ordinance) are installed. However, when either the facility used chiefly for the registration of electronic certificate users (hereafter called the "registration terminal") or the facility used chiefly for identifying the information related to users (hereafter called the "user information") and user identification codes (hereafter called the "user identification facility") is installed, the room in which the certification business facilities, except for the said registration terminal/user identification facility is not installed, is to be excluded. The following requirements are to be met. (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.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
1112			(2) Access to the certification facility room requires operation of biometric verification devices (devices employed to identify distinctive physical characteristics) by a multiple number of persons accessing the room.
1113			(3) For access to the certification facility room, certification and identification via biometric verification that the person desiring access has been authorized to do so in advance is required.
1121		(b) Control over the number of persons entering the room and identical number of persons leaving the room.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
1122			(2) Exit is completed with exit of the same number of persons who entered the room, confirming that the number of persons who exited is identical with the number of persons who entered the room.
1123			(3) After exit is complete and the certification room is empty, a motion sensor in the room will be activated to sound an alarm any movement takes place.
1131		(c)Alarm to be set off in case abnormal time is spent on operation of access control devices.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
1132			(2) Length of time required for access operation (including time the door is kept open) and number of tries are defined and registered. Length of time required for access operation is defined as length of time taking into account the number of tries executed for cross-comparison (multiple number of tries must be allowed in view of instability in biometric verification) needed to satisfy, for instance, verification accuracy (false rejection rate & false acceptance rate), biometric device cross-checking speed and verification accuracy (that is, tolerable access control operation time).

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
1133			(3) If access operation exceeds the number of tries or length of time defined and registered as in (2), alarm is set off at a location manned on 24-hour basis. Otherwise, the state of access operation is to be monitored on 24-hour basis with remote surveillance devices for immediate action in case of extraordinary behavior.
1141		(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.	(1) Items 2 through 7 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
1142			(2) Remote surveillance cameras are to be installed at positions that eliminate a "dead angle" in photographing persons entering or exiting the certification facility room or persons inside the room. If a dead-angle camera view cannot be eliminated, personnel operating the certification facilities will be trained to not position themselves in these locations and will be monitored in such a way that no one will be positioned in such a location.
1143			(3) Videotape recording devices capable of videotaping for more than one week are to be installed.
1144			(4) Persons entering or exiting the certification facility room or persons inside the said room are to be videotaped and monitored on 24-hour basis with remote surveillance devices. In addition, access detectors and remote surveillance devices are to be coordinated for automatic and continuous surveillance and videotaping when persons are entering or exiting the certification facility room or persons are present inside the said room.
1145			(5) Lapse in videotaping and monitoring should not take place in case of replacement of recording medium in videotape recording devices. If this cannot be avoided, replacement shall be done swiftly while confirming that there are no persons entering or exiting the certification facility room or persons inside the said room.
1146			(6) Video photography with remote surveillance camera and film recording is to make recorded object clearly identifiable.
1147			(7) Remote surveillance devices and videotape recording devices are to have UPS, etc., for operation in case of power failure.
1151		(ii) In a room in which a registration terminal/user identification facility is located (but that is not a certification facility room), measures (e.g., locking) are to be implemented to prevent easy access of the registration terminal/user identification facility by unauthorized personnel.	(1) Items 2 and 3 below are to be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
1152			(2) The entrance to the room in which the registration terminal/user identification facility is installed is to have a lock and key and is to be locked when no one is in the room.
1153			(3) In the room in which the registration terminal/user identification facility is installed, the location of the registration terminal/user identification facility is to be sectioned off from other facilities in order to impede easy access to the terminal/facility by persons other than authorized personnel.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		1.2 Measures Necessary to Prevent Unauthorized Access, Etc., to Certification Business Facilities	
1211	(ii) Facilities for certification business shall be equipped with the required measures to prevent illegal access via telecommunication lines, etc. (Article 4)	Measures necessary to prevent unauthorized access, etc., by means of telecommunications circuits as provided in item 2 of Article 4 of the Ordinance are to be the following .(Article 5)	(1)Items 2 through 4 below shall be defined clearly and appropriately in the administration guidelines, etc., and the facilities are to be in compliance with the standards.
1212		(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.	(2) If certification business facilities (excluding registration terminal) are linked to external network, the said facilities are to be equipped with communication devices with firewall function and network-based penetration detection function to prevent unauthorized access. Communication is to be executed via such devices.
1213			(3) Communication devices with firewall function are to satisfy the following requirements. ① Communication with unregistered protocol is to be severed. ② Origin of communication and recipient of communication are to be specified, and other communications are to be severed. ③ Communication with network business not registered is to be severed. ④ Communications processed are to be recorded.
1214			(4) Communication devices with network-based penetration detection function are to satisfy the following requirements. ① Packet communication on the network can be monitored, and unauthorized access or business obstruction attack can be detected. ② (Signature) file that signals unauthorized access, on which detection is based, can be defined manually or updated regularly with software, etc. ③ When detecting unauthorized access or signs of such an access, it is reported to the system manager
1221		(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, as well as the wiretapping and tampering of the communication contents from one component to another component.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc., and the facilities are to be in compliance with the standards.
1222			(2) If certification business facilities consist of two or more components, i.e., equipment designed for issuance and equipment designed for registration, and if these components are connected via an outside network, communication between said components must be implemented in such a way to prevent erroneous recognition of the equipment, as well as the wiretapping and tampering of the communication content.
1223			(3) If certification business facilities consist of two or more components and are installed in the same certification facility room, communication between said components must be implemented with measures that are equivalent to those specified in the example of adaptation (2) in terms of system setup, access control, internal checks, and other operational measures.
1231		(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 wiretapping and tampering of the communication content from a computer to the certification business facility.	(1) When user signature codes are created by users, if the computer systems (hereafter referred to as "facilities for receiving user identification codes, etc.") used to receive user signature verification codes, user information, and user identification codes through telecommunications lines are installed, Items 2 below shall be defined clearly and appropriately in the administration guidelines, etc., and the facilities are to be in compliance with the standards.
1232			(2) For communications sent from the facilities for receiving user identification codes, etc. to a certification business facility, measures shall be taken to prevent the erroneous recognition of these facilities, as well as the wiretapping and tampering of the communication content.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		1.3 Measures to Prevent Operation of Certification Business Facilities by Persons Without Authorization	
1311	3. Facilities used for for certification business shall be equipped with the required measures to prevent operations by parties with proper rights, and shall be equipped with functions to record operations of the concerned facilities for certification business. (Article 3)	Measures to prevent operation of certification business facilities by persons without authorization are to satisfy the following requirements.(Article 6) (i) When operating a certification business facility, the authority of each operator is to be defined the operator's authority must be able to be confirmed.	(1) Regarding those operating the certification business facilities, Items 2 through 4 below shall be defined clearly and appropriately in the administration guidelines, etc., and the facilities are to be in compliance with the standards.
1312			(2) Restrictions in access to certification business facilities can be defined by each operator.
1313			(3) Certification business facilities are to have a system in place for verifying authorized personnel by password, electronic signature, or biometrics, etc.
1314			(4) Certification business facilities connected to registration terminals are to be equipped with systems specified in Items 2 and 3 above.
1321		(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.	(1) When user signature codes are created by users and if certification business facilities are used to identify user information/user identification codes automatically, Items 2 through 4 below shall be defined clearly and appropriately in the administration guidelines, etc., and the facilities are to be in compliance with the standards.
1322			(2) In certification business facilities, user identification codes are to be be set for each user.
1323			(3) The entrance(s)/exit(s) of any room equipped with facilities for receiving user identification codes, etc. shall be outfitted with locks/keys and shall be locked when no one is in the room.
1324			(4) Certification business facilities are to have systems in place for differentiating the specific user information and user identification codes sent from the facilities for receiving user identification codes, etc., through telecommunication lines. They also are to have systems in place for confirming the specific user information and user identification codes.
1331		(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.	(1) Item 2 below is to be defined clearly and appropriately in the administration guidelines, etc., and facilities shall be in compliance with the standards.
1332			(2) Certification business facilities are to be designed in such a way as to make remote operation via network impossible, other than for handling electronic certificate issue requests from the registration terminal and the operations necessary for electronic certificate management, e.g., requests for electronic certificate revocation, etc

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
1341		(iv) The location of certification business facilities is not to be displayed.	(1) Item 2 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
1342			(2) A name, sign, or signboard that displays or suggests the location of a certification business facility is not to be posted outside or inside a structure that houses such a facility. Examples are as follows: *On the exterior of a structure that houses a certification business *At the entrance of a structure that houses a certification business *In the elevators of a structure that houses a certification business *At the entrance of a certification facility room. *At a reception desk. *In pamphlets or on website homepages, etc.
1351		(2) The functions for recording operations of certification business facilities as provided in item 3 of Article 4 of the Ordinances are as follows.	(1) Item 2 below is to be defined clearly and appropriately in the administration guidelines, etc., and facilities shall be in compliance with the standards.
1352		(i) Functions for recording the name of a requesting party (only when operated by the operator), as well as the content, date, results, etc., of each activity in the operation history.	(2) Each certification business facility is to have the following functions in place for recording daily operations. ① Identifying the person executing each activity (when an operator is involved). ② Reporting the exact location where the activity took place (e.g., a ③ Reporting the type of event (e.g., file open/close, name change, attribute change, deletion, etc.) ④ Reporting the date/time of each activity. ⑤ Reporting the results of each activity.
1361		(ii) Functions for displaying the operation history for a specific operator (only when operated by the operator).	(1) Item 2 below shall be defined clearly and appropriately in the administration guidelines, etc., and the facilities are to be in compliance with the standards.
1362			(2) A certification business facility's operations history is to be displayed for each operator.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		1.4 Encryption device employed for generation of issuer signature code	
1411	(iv) Of the certification business facilities, the electronic computers used to verify the issuer (if differentiated in accordance with the name of certification activities, the activities shall be included, hereinafter the same) of electronic certificates, and compile or manage the codes used by the issuer (hereinafter referred to as the "issuer signature codes") to comply with the criteria in Article 2 shall be exclusive electronic computers with the required functions to prevent the leakage of the concerned issuer's signature codes. (Article 4)		(1) Encryption device used for generation and management of issuer signature code (that is, computer system exclusively used for this purpose as described in item 4 of Article 4 of the Ordinances) is equipped with the following functions to curb possibility of leakage, damage, loss, etc., of the issuer signature code to the least possible minimum.
1412			① If interface exists for input/output of unencrypted encryption code, certification data, etc., and other important data in unprotected form into encryption device, the interface is physically separate from interface for other data input/output.
1413			② The encryption device is to have the following functions and at the same time have access rights restricted by function and by operator of the device. (a) Operator function: Encryption, signature, and others for implementing regular encryption functions. (b) System manager function: Functions for encryption device management, such as initializing the device and setting important parameters such as signature code.
1414			③ In order to prevent theft of issuer signature code and other data, the encryption device will have the following physical security measures implemented. (a) If the encryption device consists of independent IC chip, the chip is to be covered by non-transparent coating made of material that is sturdy and cannot be removed easily. (b) If the encryption device is covered, tamperproof measures are implemented against physical violation, such as encryption device function terminated, internal data voided, etc. (c) If the encryption device has air vent or pores on the case, measures are taken to ensure that such openings are sufficiently small and prevents probing the inside without detection.
1415			④ The following measures are to be implemented in management of issuer signature code used for the encryption device. (a) If the issuer signature codes are to be generated inside the encryption device, secure algorithm for generating pseudo-random numbers is to be used. (b) Regarding the input/output of an issuer signature code within an encryption device, said input/output is to be executed using either of the following methods. *The issuer signature codes are encrypted in input/output. *If the issuer signature codes are to be split into two or more components and input/output, it should be done directly within the encryption device. In this case, operator verification must be executed for each component of the issuer signature code. The components of the issuer signature code are to be split and united inside the encryption device. (c) If the issuer signature codes are to be stored inside the encryption device without encryption, the mechanism must be accessible externally. (d) It has the function of nullifying issuer signature codes and other security parameters when scrapping issuer signature codes.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
1421			(2) If the operating system of the computer in which the encryption device is installed is able to satisfy the following functions and requirements and to assure security comparable to security measures for the certification business facilities and for the entire certification facility room notwithstanding (1) above, it can replace such measures
1422			① Software, etc., installed to drive encryption device are installed in executable code only.
1423			② Encryption software, signature code, and other important security parameters, as well as control information, status, information, etc., are under control of the operating system equipped with functions for inspecting input/output of data.
1424			③ Operating system is equipped with functions to protect signature code, verification data, and other important security parameters from unauthorized access, etc.
1425			④ If provisions on physical independence of interface described in (1)-(1) above are not satisfied, input/output of important data is to be executed in secure method without mixing with other types of data by the operating system of the computer in which the encryption device is installed.
1426			⑤ If access right cannot be defined for each operator as described in (1)-(2) above, operator right can be defined by the operating system of the computer in which the encryption device is installed.
1427			⑥ If encryption device tamperproofing measure is any of the following, protection is to be secured by storage of the device in secure location when not in operation, monitoring with surveillance device, etc., against physical attack on the computer system, and computer operating system protection against logical attack. (a) The IC chip is covered with non-transparent coating that makes attempt at unauthorized access, etc., detectable. (b) The encryption device is covered with non-transparent case, etc., and with non-transparent coating that makes attempt at unauthorized access, etc., detectable.
1428			⑦ Regarding (1)-(4)-(b), the operating system of the computer in which the encryption device is installed does not allow input/output in methods other than that described in (1)-(4)-(b).

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		1.5 Measures necessary to prevent damages on certification business facilities from natural disasters	
1501	(v) Certification business facilities and required machines for devising measures of item 1 shall be equipped with the required measures in accordance with the level of importance of business so that they are not easily affected by natural disasters such as power failure, earthquakes, fires, and floods.(Article 4)	Measures necessary to boost resistance to damages from disasters such as power failure, earthquake, and flood, prescribed in item 5 of Article 4 of the Regulations are classified as follows and shall meet requirements specified in the corresponding items..(Article 7)	(1) Measures for protecting the certification facility room and the structure that houses it against natural and other disasters/events (e.g., power failure, earthquake, fire, flood, etc.) shall be defined clearly and appropriately in the administration guidelines, etc., and the required measures are to be implemented.
1511		(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.	(1) As earthquake preparation, the certification equipment is protected against moving and falling with either of the following means: ① Measures to prevent movement or falling are implemented with attention to installation methods recommended by certification business facility manufacturer, in view of floor response of the room in which such facilities are installed. ② Facilities are fixed to the structure with earthquakeproof supports, fall-prevention joints, etc. ③ The entire structure, floor on which certification business facilities are installed, etc., are seismic-shock-absorbent in design or certification business facility is supported by seismic-shock-absorbent platform.
1512			(2) Computer rack is protected from movement and prevention through fixture to structure, etc.
1513			(3) Components of a certification business facility that are set on racks are to be secured using fall-prevention joints, earthquake-proof straps, etc.
1514			(4) Reinforcement measures that incorporate angles, stringers, etc., are to be implemented to prevent damage on a free-access floor in the event of an earthquake.
1515			(5) Earthquake-proof measures are implemented on fixtures, supplies, etc., in the certification facility room in order to prevent earthquake damages on the certification business facilities.
1521		(ii) Certification facility room: The following requirements are to be satisfied. (a) Measures to be taken to prevent flooding.	(1) Either Item 1 or 2 is satisfied. ① Certification facility room is located on the second floor or higher in the structure. ② If certification facility room is located on the ground floor or lower, adequate measures are implemented against flood/water damage. Flooding prevention measures must especially be taken if located in sites that had sustained flood damages in the past or in sites located below sea level.
1522			(2) Waterproofing measures are taken on floor immediately above the room, such as application of asphalt or urethane waterproof paint, etc. If such measures are not possible, full-range water detectors are to be installed on beams and pillars around the floor above the room, and waterproof cover is available inside the room.
1523			(3) Certification facility room does not have wash basin, tea maker, and other water-use facilities.
1524			(4) When installing air conditioning system in the certification facility room, water control embankment or water receptacle is to be installed near the air conditioning system, with water leakage sensor installed inside either the embankment or receptacle.
1525			(5) Water leakage is monitored continuously with centralized surveillance panel, etc.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
1531		(b) Partitioning by walls	(1) The certification facility room is to be separated from other rooms with a partition or wall that is designed in such a way that it cannot be easily destroyed.
1532			(2) A certification facility room is to be designed in such a way that there is no entrance/opening that is vulnerable to invasion.
1541		(c) Installation of automatic fire detectors and fire extinguishers.	(1) Automatic fire detectors and fire extinguishers that conform with Ordinances under the Fire Defense Act and shall undergo regular inspection by fire stations, etc.
1551		(d) Installation in fire-protection areas.	(1) The area of the structure that houses a certification facility room is to be protected against fire as defined under the Construction Standards Act.
1552			(2) If a cable passes through the fire protection area, the area where the cable passes and area within 1 meter from the area are to be made fire-retardant with non-flammable materials, etc.
1553			(3) If there are ventilation, heating, or air conditioning ducts passing through the fire protection area, the area where the duct passes and area near the area are to have fire-resistant dampers.
1561		(e) Measures to be taken against power failure for power source facilities used inside the room.	(1) Uninterrupted power supply (UPS) or constant-voltage, constant-frequency (CVCF) power supply and storage batteries are to be installed for certification business facility and room access control devices used in the certification facility room
1571		(3) 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.	(1) Structure in which certification facility room is to be housed is to be located in areas not likely to be susceptible to earthquake damages. If this cannot be avoided, measures to prevent uneven subsidence in a soft foundation (e.g., pile driving), are to be implemented. Methods to control uneven subsidence are based on basic principles such as: *Compaction method: Sand compaction, vibro-flotation *Water pressure dispersion method: Gravel drainage *Pressurized dehydration method: Well point *Solidification method: Grouting, deep-strata mixing *Others: Replacement method, etc.
1581		(b) Structure to satisfy the provisions of the Construction Standards Act (No. 201 of 1950) for safety against earthquakes and relevant orders and ordinances .	(1) Structure in which certification facility room is housed to be inspected by construction project owner and comply with Construction Standards Act standards in structure strength, etc.
1591		(c) Structure to be fire-resistant or quasi-fire-resistant as provided in the Construction Standards Act.	(1) Structure in which certification facility room is housed is to conform with Construction Standards Act standards on fire-resistant structures and quasi-fire-resistant standards.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
2 Methods for verifying authenticity of users			
		2.1 Application for use of certification business, etc.	
2101	The methods provided by the ordinance of competent ministers as set forth in Article 6.1.2 of the Act are listed below: (i) Persons applying to use the certification business (hereinafter referred to as "user applicants"), shall be required to submit a copy of the Resident Record as prescribed in Article12.1 of the Residential Basic Book Act (Act No. 81 of 1968) or a Certificate of Items Stated in the Resident Record, and a copy of a family register/abstract register (applies only when submission/presentation of certificates indicating current address is required) or a Certificate of Status of Residence issued by the consulate (or director/deputy of the embassy/legation acting as consulate), or a document conforming to this as prescribed by a competent minister. Also, one or more of the following methods will be used to verifying the authenticity of the applicant. However, when implementing the approved certification business, the proxy will accept documents indicating whether the application has actually been made for the use of the certification business or the application as prescribed in (c), and a letter of proxy (if the user applicant is living outside of Japan, the letter shall conform to the country of residence) that has been signed or stamped (applies only where a certificate of stamp registration for the stamp used is provided) by the person applying for use that confirms the rights to the concerned proxy. Authentication of the proxy shall be confirmed by more than one of the methods listed below (Article 5.1.1)		(1) Items 2 through 5 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
2102			(2) The method of application for the certification business shall be defined, i.e., whether the application will be made in person, by mail, or via secure telecommunications, etc.
2103			(3) The type of document that will be used to verify the authenticity of the user and proxy as prescribed in Articles 5.1.1, 5.1.2, and 5.2 shall be defined for the specific method of application.
2104			(4) User applicants are asked to submit copies of their resident cards, Certificate of Items Stated in the Resident Record, family register or abstract register (applies only when submission/presentation of certificates indicating current address is required), certificate of status of residence issued by the consulate (or director/deputy of the embassy/legation acting as consulate), electronic certificates as prescribed in Article 3.1 of the Law on Certification Business of Local Public Organizations related to Electronic Signature (hereinafter referred to as public individual certificates), or the following documents as prescribed in the notification issued by a competent minister comforming to the above (September 8, 2015 Ministry of Internal Affairs and Communications, Ministry of Justice, Ministry of Economy, Trade and Industry Notice No. 3). ①Copy of judicial scrivener register as prescribed in the Judicial Scriveners Act (Act No. 197 of 1950) Article 8.1 (including those created as an electromagnetic record). ②Copy of land and house investigator register as prescribed in the Land and House Investigators Act (Act No. 228 of 1950) Article 8.1 (including those created as an electromagnetic record). ③Copy of notary public register as prescribed in the Notary Public Act (Act No.4 of 1951) Article 6.1 (including those created as an electromagnetic record). ④Copy of tax accountant register as prescribed in the Tax Accountant Act (Act No.237 of 1951) Article 18 (including those created as an electromagnetic record). ⑤Copy of social insurance consultant register as prescribed in the Social Insurance Consultants Act (Act No.89 of 1968) paragraph 1 of Article 14-2 (including those created as an electromagnetic record).
2105			(5) The procedure for handling the application for use by methods other than those specified shall be defined.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		2.2 Method of verifying authenticity of users, etc.	
2201	(a) The Act that requires submission of one or more of the following: A passport as prescribed in item 5 of Article 2 of the Entry and Departure Management and Refugee Approval Act (No. 319 of 1951); a residence card as prescribed in Article 19-3 of the same Act; a special permanent resident certificate as prescribed in Article 7.1 of the Special Law on the Immigration Control (Act No. 71 of 1991) for persons who have renounced Japanese citizenship based on peace treaties with Japan; licenses, permits, or a certificate of qualifications issued by the ministries/agencies listed in Separate Table; Individual Number Card as prescribed in Article 2.7 of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013); or documents used by ministries/agencies (Incorporated Administrative Agency (Incorporated Administrative Agency as prescribed in Article 2.1 of the Act on General Rules for Incorporated Administrative Agency (Act No. 103 of 1999), Local Incorporated Administrative Agency (Local Incorporated Administrative Agencies as prescribed in Article 2.1 of the Local Incorporated Administrative Agency Act (Act No.118 of 2003)), and special public corporations (set up directly in accordance with Act or corporations set up with special establishment acts in accordance with special Acts, subject to item 15 of Article 4 of Act for Establishment of the Ministry of Internal Affairs and Communications [Act No. 91 of 1999]), to certify the identification issued to their employees attached with the photograph of that specific employee. (Article 5.1.1.a)		(1) Items 2 through 11 below are to be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
2202			(2) When using a method in Article 5.1.1.a of the Ordinance to verify the authenticity of a user or proxy, the certificates and other documents issued by the specified authorities must be confirmed as genuine regarding their content, format, period of validity, etc. Further authentication will be conducted by checking the photo attached to the certificate or similar document against the person presenting the certificate.
2203	(b) Method which requires the submission of stamp registration certificate related to the stamp used to stamp the application for use (if the party applying for use is living outside Japan, the letter shall conform to the country of residence) (Article 5.1.1.b)		(3) When using a method in Article 5.1.1.b of the Ordinance to verify the authenticity of a user or proxy, the seal registration certificate must be confirmed as genuine regarding its content, format, period of validity, etc. If the official seal of the user or proxy is impressed on the application form and the seal registration certificate is attached as material to confirm identity of the user or proxy, the seal impression on the application form shall be confirmed as a match for the impression on the seal registration certificate.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
2204	(c) The method for mailing documents that inquire into the information in the application and the acceptance of replies to the inquiry shall be done via postal services that allow the post to be received only by the person to whom the document was addressed or to the person(s) designated by the sender to receive the post (hereafter referred to as "addressee). The addressee shall be required to present one of the following documents to receive the post. (1) One or more of the documents given in (a).		(4) When using a method in Article 5.1.1.c of the Ordinance to verify the authenticity of a user or proxy, the document confirming that it actually has been issued to the user or proxy shall be received.
2205			(5) In case of application by proxy and in case of acceptance of document inquiring into information in the application stipulated by Article 5.1.1.c of the Ordinance, the letter of proxy to be submitted must state clearly the content of application entrusted by the user to proxy or that acceptance will be by proxy.
2206	(2) Two or more of the following documents: insurance certificate such as health insurance, national health insurance, seaman's insurance, mutual aid association membership certificate, national pension account book, national pension, social insurance or seaman's insurance related pension certificate or mutual aid pension, military pension, etc. (3) One or more of the documents given in (2) together with one or more of the following: student card, company's identification card or qualifications certification issued by a public organization (excluding those in (a)) attached with a photo. (Article 5.1.1.c)		(6) In case of application by proxy and in case of acceptance of document inquiring into information in the application stipulated by Article 5.1.1.c of the Ordinance, the signature by the user themselves on the power of attorney form must be confirmed. At the same time, the impression of the official seal of the user affixed to the same document is confirmed to match the seal impression certified by the seal registration certificate attached to the power of attorney form.
2207	(d) The same methods as those described in a, b, and c, as approved by a competent minister. (Article 5.1.1 d)		(7) When using signed certificates to verify the authenticity of the user or proxy (limited to those issued by foreign consular offices in Japan; e.g., embassies, consulates, etc.), the validity of the signed certificates must be confirmed as to the description, format, expiry date, etc. Also, if the application form is signed by the user or proxy and the signed documents related to the signature are attached as identity verification documents of the user or proxy, the signature on the application form and that on the signed certificate attached to the application form shall be verified as the same.
2208	The method for verifying authenticity of user applicants using electronic signatures for electronic certificates for signatures they already possess, as prescribed in Article 3.1 of the Act on Certification Business of Japan Agency of Local Authority Information Systems related to Electronic Signatures, etc. (Act No. 153 of 2002). (Article 5.1.2)		(8) When using the methods of Article 5.1.2 of the Ordinance to verify user authenticity, the validity of the electronic certificate for public identification shall be confirmed in terms of description, format, expiry date, expiration status, etc. The validity of the electronic signature on the electronic certificate attached to the application also shall be verified.
2209	(2) When a user applies for a new electronic certificate for themselves, if the term of validity of that electronic certificate has expired within five years from the date of issue of the authentic, verified electronic certificate issued to that user (in accordance with the methods as described above), the issuer shall verify the authenticity of that specific user by the electronic signature on the electronic certificate currently possessed by the user. (Article 5.2)		(9)In case of confirmation of user identity when updating electronic certificate under provisions of Article 5.2 of the user employed in information for use application is verified and validity of the electronic certificate on which the said signature is attached is confirmed, such as absence of information regarding revocation. The validity of the new electronic certificate will expire in less than five years after the issue date of the electronic certificate that has authenticated the user and has been issued with any method of each Article 5.1.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
220A			(10) When users create user signature codes, if confirmation of the authenticity of the user and acceptance of the user's signature verification code are not implemented simultaneusly, confirmation that the person submitting the user signiture verification code and the user for which the confirmation of authenticity has been executed are one and the same shall be done by alotting the user identification code (information known only to the user whose identification is to be confirmed) to that specific user.
220B			(11) In case of dispute in verifying authenticity of the user or proxy, identify of the user or proxy is confirmed according to procedure established in advance and in writing.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3. Methods for other business		**3.1 Items to be explained to applicants**	
3111	(i) Important particulars on the implementation of electronic signature and use of certification business shall be explained to the applicant by appropriate methods such as the issue of documents. (Article 6)	Items to be explained to prospective users prescribed in item 1 of Article 6 of the Ordinance are to contain the following items (Article 8) (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 revocation 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.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc.
3112			(2) The following essential items shall be explained to the user clearly and concretely. ① The certification business is accredited by the relevant Minister in charge, and penalty is imposed in case of application based on falsehood which is revealed and proven. ② Electronic signature has legal force comparable to handwritten signature and seal impression, and user signature code is to be managed with due caution and confidentiality. ③ If a user signature code is compromised (i.e., a state in which it can be used by others due to theft, leak, etc.) or is likely to be put into jeopardy, or if the content of an electronic certificate is changed, or if the use of an electronic certificate is to be terminated, etc., a request for certificate revocation shall promptly be made. ④ Electronic signature algorithm used in the electronic certificate is to be that specified by the certification business in question.
3113			(3) Important information shall be explained to users by one of the following methods. ① Document issue (by mail, handed over in person, or by email) ② Explanation in person ③ Method comparable to 1 or 2.
		3.2 Items to be shown for applicants, etc.	
3211	(ii) In order to verify the applicant's intentions related to application, the applicant shall be asked to submit application form on use or other documents with the user's signature or stamp (applies only when the seal registration certificate of the stamp used is attached) or send information related to the application for use (only those to which the electronic signature is implemented and which is acknowledged with the electronic certificate provided by certification business to be accredited (hereinafter referred to as the "accredited certification business".) or any operation similar thereto). (Article 6)	User application and other written or application-related information in item 2 of Article 6 of the Ordinance shall show or contain in recording the following items. (Article 9) (i) The name, address, and date of birth of the applicant	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc.
3212		(ii) Specific uses of the electronic certificate for which application was submitted. (iii) The name of the applicant for use in Rōmaji (Roman letters). (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 verifying authenticity of the user (excluding cases in which information on application is to be transmitted).	(2) The application form or information related to the application for use shall contain the following: ① The user's name, address, and date of birth. ② The purpose of the electronic certificate used for the application. ③ The name of the applicant for use in Rōmaji (Roman letters). ④ 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 verifying authenticity of the user (excluding cases in which information on application is to be transmitted)
3213		(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 verifying authenticity of the proxy), and reason for application by proxy.	(3) In the event of application by proxy, in addition to (2), the application form shall be signed by the proxy or stamped using the registered seal certified by the seal regisration certificate of the proxy (only when a seal registration certificate is used as the method for verifying authenticity of the proxy) and the reason(s) stated for application by proxy.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.3 Measures necessary for generation of user signature code by certification business	
3301	(iii) In the event the certification business provider creates the codes (hereinafter called the "user signature codes") that users will use to sign an electronic signature, the certification business provider must issue or send the user signature code to each specific user via a safe and accurate method. They also must promptly delete the specific user signature codes and any copies of them. (Article 6)		(1) So that the certification business provider can generate a user signature code, Items 2 through 5 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3302			(2) The user signature code is to be generated by multiple persons and measures are to be taken to prevent tapping, alteration, and/or other incidents by controlling access rights, conducting internal checks, etc., in the certification business facility room or in an environment in which comparable safety has been secured.
3303			(3) When transferring, outputting, etc., user signature codes, measures shall be taken to prevent tapping, alteration, and/or other incidents by controlling access rights, conducting internal checks, etc., in the certification business facility room or in an environment in which comparable safety has been secured.
3304			(4) When PINs, etc., used to activate the user's signature code are generated, transfered, and outputted, measures shall be taken to prevent tapping, alteration, and/or other incidents by controlling access rights, conducting internal checks, etc. In addition, after removing PINs, etc from devices used for generating, transferring, outputttting, etc. then, PINs, etc. used for activating user signature codes must be completely discarded or erased without delay.
3305			(5) The generated user signature code shall be provided to the specific user via a safe, secure method, and the user must provide a receipt that has been signed by that user with a signature that identifies the user, or stamped with a seal that identifies the user, or electronically signed by that user

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3311	When the user creates a user signature code and the certification business provider receives the user signature verification code that corresponds to that specific user signature code via telecommunication, the user identification code (a one-time code to identify a specific user that has been created in such a way as to not be easily guessed) shall be sent to the user via a safe and reliable method. This code must not be revealed to anyone other than the specific user until it has been used to identify that user. (item 3-2 of Article 6)		(1) When the user creates a user signiture code and the certification business facility is automatically operated by identifying the user information and user identification code, and if the certification business provider receives the user signature verification code that corresponds to that specific user sigunature code via telecommunications, Items 2 through 6 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented. However, Item 5 shall include the provision that the certification business facility is not to be operated automatically by identifying the user information and the user identification code.
3312			(2) The user identification code must be created using a safe, pseudo-random, number generating algorithm 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.
3313			(3) The user identification code must be sent to the user via a safe and reliable method. When electronic certificates are issued to a specific user, receipt of the user identification code must be verified.
3314			(4) The user identification code must be stored using methods such as encryption, etc., in a certification business facility room or equivalent environment that ensures safety.
3315			(5) When sending a user identification code, the user must verify the facilities for receiving user identification codes, etc., and implement measures to prevent tapping and/or alteration of the communicated data.
3316			(6) Measures to prevent a user identification code from being used for identification processes thereafter must be implemented immediately (i.e., measures to prevent the use of a user identification code that corresponds to the user identified in the certification business facility through discarding or flagging as "used").

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.4 Items related to electronic certificate	
3401	(iv)Term of validity of electronic certificates shall not exceed five years.(Article 6)		(1) Item 2 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3402			(2) The period of validity of an electronic certificate issued to a user shall be less than five years from the date of determination for issuance.
3411	(v) Electronic certificates should list the following particulars. (Article 6) (a) Name and issue number of issuer of concerned electronic certificate. (b) Date of issue of concerned electronic and term of validity. (c) Name of user of concerned electronic certificate.		(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3412	(d) Identifiers of user signature verification codes related to concerned electronic certificate and algorithms related to concerned user signature verification codes.		(2) The format and language of the electronic certificate issued to the user shall be prescribed and the certificate shall contain the following information. ① Name of issuer (including type of business if engaged in various types of certification business) ② Issue number (to be unique in the certification business, including the accredited certification business in question) ③ Period of validity showing starting date to termination date (including hour, minute, and second). ④ Name of user ⑤ User signature verification code and algorithm ID related to the verification code
3413			(3) If the user creates a user signature code, the user signature verification code recorded in the electronic certificate as stipulated in Item 5 (d) of Article 6, of the Ordinances shall be confirmed to have a corresponding user signature code. This will be done by employing methods to verify an electronic signature executed with a user signature code by using the user signature verification code in question. In addition, when verifying a specific user signature verification code, the key length and cryptgraphic algorithm shall be checked.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3421	(vi) Electronic certificates should be equipped with issuer verification measures which conform to the criteria set forth in Article 2. (Article 6)	The electronic signature system that satisfies the criteria set forth in Article 2 of the Ordinance shall be any of the following:(Article 3)	(1) Item 2 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3422		(i) RSA/SHA-1(object identifier 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 identifier 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(object identifier 1 2 840 10040 4 3) with modulus consisting of elements of 1,024 bits.	(2) The electronic signature system used in issuing electronic certificates is to employ any of the following: ①RSA/SHA-1(object identifier 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 composit numbers of more than 1,024 bits. ②RSA-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 composit numbers of more than 1,024 bits. ③ECDSA/SHA-1(object identifier 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. ④DSA/SHA-1(object identifier 1 2 840 10040 4 3) with modulus consisting of elements of 1,024 bits.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.5 Measures to prevent error in recognition between accredited certification business and other business	
3511	(vii)Appropriate measures should be taken to prevent erroneous recognition between accredited certification business and other business by the user or others. (Article 6)	Appropriate measures to prevent erroneous recognition between accredited certification business and other business by the user or others prescribed in item 7 of 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: (Article 10)	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3512		(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.	(2) Uses of the issuer signature code is restricted to signature on electronic certificate issued for the certification business in question. Uses of the issuer signature code other than the above are restricted to the following. ① An electronic signature on mutual certification with a certification business provided by national or local governments in compliance with standards comparable to or exceeding other accredited certification businesses. ② An electronic signature on electronic certificate of the certification business in question (own signature). ③ An electronic signature on new electronic certificate for certification business in question for updating issuer signature code in question. ④ An electronic signature on old electronic certificate for certification business for updating issuer signature code in question. ⑤ An electronic signature on electronic certificate issued to certification business facilities or person operating such facilities. ⑥ An electronic signature on magnetically recorded information about revocation. ⑦ An electronic signature on electronic certificate issued to facility for disclosure of electronic certificate revocation information and information on the certification business in question.
3513		(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	(3) A record is kept of the value determined by converting with one or more of SHA-1,SHA-256,SHA-384 or SHA-512 the value in the electronic certificate related to the issuer's signature verification code corresponding to the issuer's electronic code. When the particular operation begins, the information is disclosed as tamper-proof.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.6 Record of attributes in electronic certificate	
3601	(viii) When recording the user's title and other attributes (excluding the user's name, address, and date of birth) on the electronic certificate, appropriate measures should be taken to prevent erroneous recognition by the user or others that the certification of the concerned attributes are related to the accredited certification business.(Article 6)		(1) If the user's title or other attributes shall be recorded on the electronic certificate, Item 2 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3602			(2) It must be noted on the electronic certificate that the user's title and other attributes (excluding the user's name, address, and date of birth) recorded on the electronic certificate are excluded from certification in accordance with the Electronic Signature Act (Act on Electronic Signature and Certification Business) or a link to the information must be included on the electronic certification.
		3.7 Providing information to parties seeking signature verification	
3711	(ix) The signature verifier (receives information from the user that electronic signature was performed, and verifies that the concerned user performed the concerned electronic signature, hereinafter the same) should have easy access to the codes used for verifying the issuer of the electronic certificate (hereinafter referred to as the "issuer signature verification code") and other necessary information. (Article 6)	Information necessary as provided in item 9 of Article 6, of the Ordinance shall contain the items described as follows: (Article 11) (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 revocation of the electronic certificate is not recorded.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3712			(2) Items describing the signature verifier, including the following Items ① through ③, must be described in such a way that they can be clearly understood, and the location of the link to the electronic certificate must be included. ① The issuer's signature verification code and fingerprint must be properly obtained and the electronic signature by the issuer of the electronic certificate must be verified, in order to verify the issuer of the electronic certificate. ② The purpose of use or the scope of the application of the electronic certificate, or the restrictions thereof (including requirements for use notified to user) must be confirmed. ③ Confirmation of whether an electronic certificate revokes shall be done using appropriate methods.
3713			(3) The signature verifier must be able to easily obtain Items ① to ③ below that are required to confirm the information described in (2) via links on the electronic certificate. ① Electronic certificate and fingerprint of the issuer ② Documents describing the purpose of use or the scope of the application of the electronic certificate, or the restrictions thereof (including requirements for use notified to user). ③ Revocation information for an electronic certificate.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.8 Items on electronic certificate revocation	
3801	(x) In the event the user requests that the electronic certificate be revoked or discovers a fAct in the particulars recorded on the electronic certificate within the term of validity, the date of revocation of the concerned electronic certificate and other information on revocation should be recorded by electromagnetic methods promptly (electronic method, magnetic method, or other methods which cannot be recognized by perception of others, hereinafter the same). (Article 6)		(1) Items 2 through 5 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3802			(2) Reason(s) for the revocation of an elecronic certificate by the user, etc., and reason(s) for revocation by the certification business provider shall be clearly defined.
3803			(3) The revocation request method, the document required for the revocation request, and the described items shall be defined.
3804			(4) If an revocation request is accepted, the method for verifying the authenticity of the applicant, the procedure for recording information related to the revocation, etc., shall be defined and the measures associated with the revocation are to be immediately implemented.
3805			(5) The format of revocation information recorded electromagnetically, the content of the revocation informaion, and the updating cycle shall be clearly defined.
3811	(xi). The signature verifier should be able to easily verify information on the revocation of the preceding item by the method which automatically sends the information when requested by the signature verifier and other methods within the term of validity of the electronic certificate. (Article 6)		(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3812			(2) One of the following methods must be used so that the signature verifier is able to easily confirm the revocation information for an electronic certificate during the time frame that certificate is valid, as indicated on the certificate. ① Disclosure of electronic certificate revocation list showing certificates that have been revoked ② Confirmation of state of electronic certificate revocation based on on-line certificate status confirmation protocol ③ Other methods comparable in function to Items ① or ② above.
3813			(3) The method of inquiry by the signature verifier, if the validity of an expired electronic certificate is to be defined.
3821	(xii) When information on the revocation of the electronic certificate is recorded pursuant to the provision of item 10, the user of the concerned electronic certificate should be notified of this promptly. (Article 6)		(1) Item 2 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc.
3822			(2) In the event of revocation of an electronic certificate, the user of that electronic certificate must be immediately notified.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.9 Ordinances on management of certification business	
3901	(xiii) The contact of the certification business, business conditions, and other provisions on the implementation of certification business should be appropriately prescribed, the concerned provisions should be recorded by a electromagnetic method, and the user and other parties should be able to easily read the concerned provisions by a method which automatic sends the information when requested by the user or other parties or other methods. (Article 6)	(1) Regulations on execution of certification business as provided in item 13 of Article 6, of the Ordinance shall contain provisions shown in the following items: (Article 12)	(1) Items 2 through 13 below shall be defined clearly and appropriately in the certification business rules, and recorded and disclosed electromagnetically.
3902		(i) Name and contact address of the certification business provider (address, telephone number, facsimile number, and electronic mail address)	(2) Name and address of the certification business provider *Address of the certification business provider (including postal code, name of prefecture, name of building, floor, etc.) *Name of contact office *Telephone number (including the certification business provider's number and area code) *Business hours *Facsimile number (including the certification business provider's number and area code) *Email address
3903		(ii) Restriction items when restrictions apply to objective, target, and range of certificate use.	(3) Items on purpose, target, and restrictions on certification ① Party to which electronic certificate is issued by the certification business in question ② Purpose and restrictions on use and other relevant items on electronic certificate issued by the certification business in question ③ Method for confirming that the user attributes (excluding user name, address, and date of birth) shown on the electronic certificate outside the scope of the certification of the Electronic Signature Act (Act on Electronic Signature and Certification Business).
3904		(iii) Restriction items if restrictions apply to range of guarantee and responsibility to be taken	(4) Scope of guarantee and immunity restrictions, if any. ① Guarantee or responsibility of the certification business provider ② Scope of guarantee and immunity restrictions
3905		(iv) Items on methods of verifying authenticity of the user and method of user application	(5) Items on verifying authenticity of the use application and user. ① Method of application for the electronic certificate and required documents ② Method of verifying the authenticity of the user and documents to be used to verify their authenticity, etc.
3906		(v) Items on requesting revocation of electronic certificate	(6) Items on the request for the revocation of an electronic certificate ① Method of the request for the revocation ② Items to be recorded and required to be recorded in written request for the revocation or request information ③ Reason(s) for electronic certificate revocation (including those from the certification business provider) ④ Method of verifying authenticity of requesting party
3907		(vi) Items on method of confirming information on revocation of electronic certificate and period for confirmation	(7) Method of confirming the revocation information for an electronic certificate and items on period of validity ① Information about the revocation to be disclosed, the method of disclosure, and the cycle of updates to the revocation information of an electronic certificate. ② Method of giving notice to users of electronic certificates regarding revocation ③ Method for dealing with an inquiry from a signature verifier regarding information about the revocation of an electronic certificate after the expiration of that certificate.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3908		(vii) Items on security in certification business (including items on handling private information on the user)	(8) Items on security ① Matters regarding security management in the certification business ② Matters regarding handling personal information
3909		(viii) Items on fees related to use of certification business	(9) Items on fees ① Charges required for the use of the certification business and payment methods, etc., or where this information can be found
390A		(ix) Items on preservation of books and	(10) Items on preservation of books and documents ① Preservation period and method, etc., for important books and documents to be stored by the certification business
390B		(x) Items on termination of business	(11) Items on termination of business ① Revocation method for an electronic certificate that already has been issued and the timing and method for notifying users in the event that business is terminated.
390C		(xi) Acts and Ordinances applied in case of dispute between certification businesses providers and items on procedure for resolution	(12) Act and Ordinances applied in case of dispute between certification business provider and relevant parties and items on procedure for settlement ① Act and Ordinances applied in case of dispute between certification business provider and relevant parties regarding certification business (in principle, Japanese domestic act, etc.) ② Procedure for dispute resolution, court of jurisdiction, etc.
390D		(xii) Items on revision of relevant Ordinances and items on notification method of users and other	(13) Provisions in revising the Ordinances and items on notification method ① Operation procedures and approval for revision of the Ordinances ② Notification method users and other persons in the event of revision of the Ordinances

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.10 Termination of certification business	
3A01		(2) Provisions listed in item 10 in the preceding paragraph shall also apply to report to users for termination of accreditation-related business no later than 60 days prior to the termination (on the date of expiration of certification business in the event an accreditation extension has not been sought) (although not applicable under unavoidable circumstances such as invalidation of accreditation under Article 14.1 of the Act) and for revocation procedure for electronic certificate issued to user by date of termination of the accredited certification business..(Article12)	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3A02			(2) When terminating an accredited certification business, including in the event an accreditation extension has not been sought, the users must be notified of termination of the certification business no later than 60 days prior to the termination.
3A03			(3) The electronic certificates of all users issued by the concerned accredited certification business must be revoked by the date of termination of the accredited certification business, and the method of verifying the information related to the revocation after the termination must be defined and implemented.
		3.11 Information disclosure to owner of electronic certificate	
3B01	(xiv) In the event the person recorded as the user in the electronic certificate reports of the infringment of rights or interests, or the risk of invasion, the documents indicated in Article 12.1.1 b and c on the user related to the concerned electronic certificate should be disclosed to the person making the report promptly in response to the request. (Article 6)		(1) Item 2 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3B02			(2) In the event the person recorded as the user of an electronic certificate reports an infringment of rights or interests, or the risk of an infringment , the following items shall be defined and implemented if the required information is disclosed. ① Documents required for reporting and the reporting method ② Method for verifying authenticity when receiving the report ③ Information to be disclosed (the application form of the electronic certificate, the documents used for verifing the authenticity of the user, the data recorded on the electronic certificate, etc.)

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.12 Organization, etc., for management of certification business	
3C01	(xv) The following items should be prescribed clearly and appropriately, and business should be implemented appropriately based on the concerned particulars.		(1) Regarding the procedure(s) for business being carried out according to the responsibilities and scope of authority of each worker in the certification business, and Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
3C02	(a) Procedure of business		(2) In the event of change(s) in the procedure(s) of the certification business, the change(s) shall be recorded promptly in the administration guidelines, etc.
3C03			(3) Training programs on the certification business procedure(s) shall be developed and implemented according to the scope of responsibility and authority of each worker involved in the certification business. Moreover, appropriate training shall be implemented in the event that the certification business procedure(s) change.
3C11	(b) Responsibility, rights, and chain of commands and orders of the persons providing business		(1) Responsibility, authority, and chain of command of the persons involved in the certification business and Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc.with attention to internal job jurisdiction.
3C12			(2) In the event of change(s) in responsibility, authority and chain of command, the change(s) shall be recorded promptly in the administrative guidelines.
3C13			(3) Training programs on the responsibility, authority and chain of command for each worker involved in the certification business shall be developed and implemented according to the scope of responsibility and authority of each worker involved in the certification business. Appropriate training shall be implemented in the event the responsibility, authority and chain of command of each worker involved in the certification business change.
3C21	(c) In the event of entrusting part of business to others, the scope of business entrusted. Details, method of managing the management of the concerned business by the entrusted party, method of ensuring the appropriate implementation of concerned business.		(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented. When business is entrusted, the scope is limited to a portion of the business. This portion of the business includes the business related to verifying the authenticity of users, the business related to certification business management and administration, and the business related to the storage of books and documents, etc.
3C22			(2) In the event of consignment agreement, procedure(s) related to the business consignment and content of the business contracted shall be defined clearly, with strict compliance with entrustor instructions, definition or responsibilities, guarantee, etc., to be clarified, as well.
3C23			(3) Proper business management shall be ensured by monitoring through regular reports, etc., from the contractor on the business consigned.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3C31	(d) Particulars on the auditing of business		(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3C32			(2) Audit standards for the certification business shall be defined (i.e., the standards for confirming the appropriate administration in accordance with the procedures, etc., defined in item 13 of Article 6, and item 15-a of Article 6 of the Ordinance), and regular audits shall be implemented.
3C33			(3) Measures including the review of facilities, ordinances, etc., shall be implemented in accordance with audit results, updates in security technology and any additional requests in the audit report, and the results shall be evaluated.
3C41	(e) Allocation of persons with adequate knowledge and experience on the technologies related to business		(1) Item 2 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
3C42			(2) The number of engineers with the knowledge and experience necessary to the execution/administration of electronic signature technology/key management technology, as well as security for the administration of certification business, shall be defined and allocated as workers in the certification business.
3C51	(f) Measures required to prohibit the use of the accessed information for purposes other than those intended when verifying authenticity of the user, and to prevent the leakage, loss, or damage of the contents of books and documents listed in each items of Article 12.1.		(1) Items 2 through 4 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3C52			(2) Handling and protection of personal information shall be defined, storage location(s) shall be secured, and personal information submitted by users shall be managed appropriately.
3C53			(3) At application for the electronic certificate, the handling of personal information and scope of information entry in the certificate shall be presented clearly to the user and approved by the user.
3C54			(4) Training programs on the handling and protection of personal information appropriate to role shall be developed and implemented for each employee involved in the certification business.
3C55			(5) Storage of books and documents defined in each item of Article 12.1 of the Ordinances, including Items in (6) below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3C56			(6) The following measures shall be implemented to prevent the leakage, loss, or damage of each record. ① Common requirements *Each record is to be stored in a room with a door that can be placed under lock and key and separated by partition or wall, etc. *Room in which records are stored is to be equipped with automatic fire detectors and extinguishers. *Records are to be kept in a place away from direct sunlight or insulated to prevent exposure to direct sunlight. ② Documents and information on paper shall be stored in the original *Environment developed to prevent original record from not becoming *Kept in customized files. ③ Additional requirements for records to be stored in electromagnetic * The computers and peripherals, operating systems, and applications shall be maintained and stored to allow the contents of the recording media to be displayed. If any computer, peripheral, operating system, or application is to be upgraded, then the personnel concerned must take measures to ensure its compatibility with the particular recording media and prevent display failures. * Recording media shall be stored in an appropriate case, etc., to prevent failure of data display. Measures shall be taken to ensure recording according to the characteristics of each medium. However, measures that do not compromise the entirety and confidentiality of the content must be taken.
3C61	(g) Particulars on risk management		(1) Items 2 through 5 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3C62			(2) Measures in the event of compromise to or possible compromise to of the issuer's signature code and the recovery procedure shall contain the following. ① Revocation of electronic certificates issued to all users by the specific certification business. ② Notification to the electronic certificate users, disclosure to the verifying parties, and the methods used ③ Study into cause and damages and measures specific to cause ④ Notification to relevant Minister
3C63			(3) Measures damages caused by natural disaster, etc., with termination of business and operation and recovery procedure are to contain the following. ① Notification to the electronic certificate users, disclosure to the signature verifier, and the methods used ② Study into cause and damages and measures specific to cause
3C64			(4) If there is compromise or possible compromise to the issuer signature code; e.g., disasters or breakdown of certification equipment or any other event that would result in suspension of the ability to provide information regarding revocation to the signature verifiers for any length of time exceeding that stipulated in the certification ordinances, and that the signature verifier has no means of learning about the suspension, the contents of the problem, the date and time of occurrence, measures, and other matters that have been confirmed must be disclosed promptly to the relevant minister.
3C65			(5) Training programs on the measures and recovery procedures for problems resulting from compromise to the issuer signature code, or from disasters, etc., shall be planned and implemented according to the scope of responsibility and authority of each employee involved in the certification business.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.13 Authorization, etc., on operation, etc., of certification business facilities	
3D11	(xvi) The inspection of the room installed with the facilities for the concerned certification business, approval of related operations, and management of identification codes related to the concerned approval should be appropriately implemented in accordance with the degree of importance of the business implemented at the facilities for certification business. (Article 6)	Permission for access to room where certification business facilities are installed and operation of such facilities under item 16 of Article 6, of the Ordinance and appropriate management of the identification code related to such permits shall be implemented by satisfying the following (i) Access to the certification facility room is to be executed in multiple number of persons only.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3D12			(2) Designation and registration of the persons authorized to enter the certification facility room shall be conducted, and access to the room shall be executed in multiple number of persons only.
3D13			(3) Continuous surveillance is conducted whether the person enter the certification facility room in the defined access method and procedures.
3D21		(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	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3D22			(2) In the event that an unauthorized persons must be allowed into the certification facility room, they must be escorted by multiple number of persons who are authorized to have access to the room.
3D23			(3) Continuous surveillance is conducted whether the persons not authorized enter the certification facility room in the defined access method and procedures.
3D31		(iii) Identification code for the system manager shall be placed under exceptionally strict control.	(1) If access control to the certification business facility is controlled with passwords, Items 2 and 3 below shall be defined clearly and appropriately in the administration guidelines, etc., and implemented.
3D32			(2) The procedure for and management of user account password settings and changes, including regular revisions, etc., shall be carried out. In addition, electronic records of passwords, such as password files, must be encrypted and accessible only by authorized personnel.
3D33			(3) The account password for the system manager shall be strictly controlled by the inclusion of special characters distinguished from Item (2) above, as well as a shorter update cycle, the prohibition of password changes via remote control, etc.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
		3.14 Measures necessary to prevent leakage of issuer signature code	
3E11	(xvii) Measures should be taken to prevent the creation and management of issuer codes by several persons, and the leakage of other concerned issuer signature codes. (Article 6)	Measures necessary to prevent leakage of issuer signature code provided in item 17 of Article 6 of the Ordinance shall satisfy the following requirements: (Article 14)	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3E12		(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 of Article 4 of the Ordinance.	(2) Issuer signature code is to be generated by a multiple number of persons and cannot be generated by only one in the group.
3E13			(3) Generation of the issuer signature code shall take place in the certification facility room using an encryption device.
3E21		(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 of 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).	(1) Items 2 through 4 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3E22			(2) Backup copies of the issuer signature code are to be executed in the certification facility room by a multiple number of persons and cannot be generated by only one in the group.
3E23			(3) If issuer signature code backup is done by using duplication feature of the encryption device, the following requirements are to be satisfied ① The encryption device executing backup is to be kept in the certification facility room or in a location with a comparable level of security.
3E24			(4) If issuer signature code backup is not done by using duplication feature of the encryption device, secret dispersion is adopted, and the following requirements are to be satisfied. ① The scattered codes are to be stored with access control by lock and key, etc., to deny contact by unauthorized persons and with measures executed to prevent fire. ② The scattered codes are to be kept in different locations.

Item	Implementation Ordinance	Guidelines	Conformity with the Accreditation criteria
3E31		(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.	(1) Item 2 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3E32			(2) To change an issuer signature code, the following requirements must be met. ① The change shall be executed inside the certification facility room. ② The change procedure shall involved multiple personnel and shall be done using a method that cannot be performed by only one person.
3E41		(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.	(1) Items 2 and 3 below shall be defined clearly and appropriately in the certification business rules and administration guidelines, etc., and implemented.
3E42			(2) To discard issuer signature code (including backup), any of the following method is to be employed and executed by a multiple number of persons to confirm that it is destroyed irreversibly. ① physical destruction ② complte initialization ③ Other ways to assure that all issuer signature codes to be destroyed are destroyed irreversibly.
3E43			(3) The issuer signature code and backup copies of the code (including the code that has been reproduced and dispersed) shall be discarded immediately in accordance with a specific procedure.

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
4 Books and documents		**4.1 Books and documents, etc. related to the application for certification business**	
4101	Those books and documents relating to the application for the use of authentication operation as described below (Article 12.1.1) must be kept for 10 years after the expiration of validity of the electronic certificate relating thereto (Article 12.2). Such books and documents (only those documents on which no signature or seal of the user or proxy is affixed) may be stored in electromagnetic recording media (Article 12.4). Those books and documents to be stored must be the original thereof (except those documents provided in the preceding paragraph) (Article 12.5). (a) Records relating to the explanation in item 1 of Article 6 (Article 12.1.1(a))	(1) The records relating to the explanation described in item 1 of article 6 are created and preserved. (The explanation shall be given to the applicant as to the important matters relating to the method of implementing electronic signatures and the use of an certification business by delivering relevant documents or any other appropriate method.) Such records include any additional information relating to the date of implementation thereof and the identification of the person who implemented it	Records of explanation given to the user Examples: * User agreement * Written consent for matters explained
4102	(b) Application for use (Article 12.1.1)	(2) The documents or information relating to the application submitted by the user of its proxy (only those to which the electronic signature is implemented and which is acknowledged with the electronic certificate provided by accredited certification providor or any operation similar thereto, including records for which the validity of the electronic signature is confirmed) are preserved. Such documents or information include any additional information relating to the date of receipt thereof and the identification of the person who received them.	Documents or information relating to the application for use. Examples: * Application for use (including power of attorney in the case of an application by proxy) * Information related to the application for use by electronic signature and validation confirmation records
4103	(c) Copies of documents or certificates submitted to the certification business provider to confirm the authenticity of the user (Article 12.1.1(c))	(3) Copies of documents and certificates relating to the application for use submitted for confirmation of authenticity of the user or proxy or any information relating thereto (only those to which the electronic signature verified by the electronic certificate provided by accredited certification providor or any operation similar thereto is implemented, including records for which the validity of the electronic signature is confirmed) are preserved. Such copies of documents and certificates or any books relating to the management thereof include any additional information relating to the date of receipt thereof and the identification of the person who received them.	Documents submitted for confirmation of authenticity Examples: * Copy of residence certificate * Proof of personal seal registration * Authenticity verification management book relating to the user and its proxy * Official personal certificate and validity check records used for an electronic signature
4104	(d) Name of the person who determines the approval or denial of the application for use (Article 12.1.1(d))	(4) The name of the person who determines the approval or denial of the application for use and the date of such determination are recorded, and such record is preserved.	Name of the person who determines the approval or denial of the application Examples: * Electronic certificate issue instruction
4105	(e) In the event the application for use is not approved, the documents that describe the reason therefor (Article 12.1.1(e))	(5) In the event the application for use is not approved, the documents that describe the reason therefor are prepared and preserved.	Books that describe the reason for not approving the application Examples: * Electronic certificate issue instruction * Copy of notice describing the reason for rejecting the issuance
4106	(f) Electronic certificate and records relating to the creation thereof (Article 12.1.1(f))	(6) The electronic certificate and any records relating to the creation thereof are prepared and preserved. The foregoing records include any additional information relating to the date of implementation thereof and the identification of the person who implemented such operation as well as the person who is responsible for such operation.	Electronic certificate and electronic certificate issuance management book

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
4107	(g) Issuer signature verification code (Article 12.1.1(g))	The issuer signature verification code-related records are preserved. The foregoing records include any additional information relating to the date of implementation thereof and the identification of the person who implemented such operation as well as the person who is responsible for such operation.	Issuer electronic signature or issuer signature verification code and production records Examples: * Issuer electronic certificate generation instructions (production request and reception) * Issuer electronic certificate generation work management book
4108	(h) Records relating to the generation and management of the issuer signature code (Article 12.1.1(h))	(8) The records relating to the generation and management of the issuer signature code are prepared and preserved. ① The records relating to the generation and management of the issuer signature code include those relating to the following: (a) Provisions stipulating the scope of use of the issuer signature code; (b) Generation and preservation of the issuer signature code (backup-related) (c) Change in the settings of certification business facilities which makes the use of the issuer signature code possible or impossible; (d) Backup of the issuer signature code; (e) Restoration of the issuer signature code; (f) Abolishment of the issuer signature code. The foregoing records (except (a)) include any additional information relating to the date of implementation thereof and the identification of the person who implemented such operation as well as the person who is responsible for such operation.	Records relating to the generation and management of the issuer signature code Examples: Books relating to the generation and management of the issuer signature code
4109	(i) In the event the certification business provider generates the user signature code, the records relating to the generation and abolishment of such user signature code and the receipts from the user (Article 12.1.1(i))	(9) ① In the event the certification business provider generates the user signature code, the records relating to the generation and abolishment of such user signature code are prepared and preserved. The foregoing records include the records relating to the distribution as well as any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation and the person who is responsible for such operation. ② The receipts from the user or any information relating thereto are preserved (only those to which the electronic signature is implemented which is acknowledged by the electronic certificate provided by accredited certification providor or any operation similar thereto, including records for which the validity of the electronic signature is confirmed). The foregoing records include any additional information relating to the date of receipt thereof and the identification of the person who received them.	① Books related to the generation and deletion of a user signature code. Examples: * User signature code generation/deletion management books ② Receipts from the user Examples: * Receipts * Receipts management books

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
		4.2 Books and documents, etc. related to the revocation of an electronic certificate	
4201	The books and documents relating to the revocation of an electronic certificate as described below (Article 12.1.2) must be preserved for the period of 10 years after the expiration of validity of an electronic certificate relating to such books and documents (Article 12.2). Such books and documents (only those documents on which no signature or seal of the user or proxy is affixed) may be stored in electromagnetic recording media (Article 12.4). Those books and documents which are stored must be the original thereof (except those documents provided in the preceding paragraph) (Article 12.5). (a) The written requests for invalidation and other records relating to the determination of invalidation (Article 12.1.2(a))	(1) The written requests for invalidation of an electronic certificate and other records relating to the determination of invalidation are preserved (including those materials that are used for the verification of authenticity of the person who requested the invalidation of the electronic certificate). The foregoing records include the reasons for the invalidation. The foregoing written requests for invalidation of an electronic certificate or any information relating thereto (only those to which the electronic signature verified by the electronic certificate provided by accredited certification providor or any operation similar thereto is implemented, including records for which the validity of the electronic signature is confirmed) are preserved and other records relating to the determination of invalidation include any additional information relating to the date of receipt thereof and the identification of the person who received them.	Written requests for revocation and other records relating to the determination of revocation (including the reasons for revocation) Examples: * Written request for the revocation of an electronic certificate * Materials to confirm the authenticity of the person in question or the proxy * Information on the request for the revocation of an electronic certificate with an electronic signature affixed and the electronic certificate for public identification, along with validation confirmation records * Request for revocation and authenticity verification implementation management book (written confirmation) * Revocation instruction
4202	(b) Name of the person who determines the revocation of an electronic certificate (Article 12.1.2(b))	(2) The name of the person who determines the revocation of an electronic certificate and the date when such revocation is determined are recorded, and such records are preserved.	Name of the person who determines the revocation Examples: * Revocation instruction * Revocation procedure management book
4203	(c) In the event the request for revocation of an electronic certificate is rejected, the documents that state the reasons therefore (Article 12.1.2(c))	(3) In the event the request for revocation of an electronic certificate is rejected, the documents that state the name of the person who makes the determination thereof, the date when such determination is made, and the reasons therefore are prepared and preserved.	Reasons of rejection of revocation request Examples: * Written decision of rejection of revocation request * Revocation procedure management book * Copy of notice of reason for rejection of revocation request
4204	(d) Information relating to the revocation defined in item 10 of Article 6 and the records relating to the preparation thereof (Article 12.1.2(d))	(4) The information relating to the revocation defined in item 10 of article 6 of the ordinance and the records relating to the preparation thereof are prepared and preserved. In the event the request for invalidation of an electronic certificate is made by the user or any matters that are not based on the facts are discovered in the records stated in the electronic certificate within the validity term of an electronic certificate, the date of invalidation of such electronic certificate and other information relating to the invalidation shall be promptly recorded by electromagnetic method (means any electronic method, magnetic method and other method that can not be recognized by human The foregoing records include any additional information relating to the date of implementation thereof and the identification of the person who implemented such operation and the person who is responsible for such operation.	Any and all information on revocation (CRL, etc.) Examples: * Revocation instruction * Revocation procedure management book

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
		4.3 Books and documents, etc. related to the organizational management of the certification business provider	
4301	The books and documents relating to the organization management of the certification business provider as described below (Article 12.1.3) must be preserved for 10 years after the expiration of validity of an electronic certificate relating to such books and documents (Article 12.2). Such books and documents (only those documents on which no signature or seal of the user or proxy is affixed) may be stored in electromagnetic recording media (Article 12.4). Those books and documents to be preserved must be the original thereof (except those documents provided in the preceding paragraph) (Article 12.5). (a) Regulations defined in item 13 of Article 6 and the records relating to the amendment thereof (Article 12.1.3(a))	(1) The regulations described in item 13 of Article 6 of the Ordinance and the records related to the amendment thereof shall be prepared and preserved. (The contact information, terms and conditions of provision of authentication operation, and other provisions on the implementation of authentication operation shall be appropriately determined, and such provisions shall be recorded by electromagnetic method that allows automatic transmission thereof or otherwise if requested by the user and other parties so that the user and other parties are able to access easily to such provisions.) The foregoing records include any additional information relating to the date of implementation thereof and the identification of the person who implemented such operation and the person who is responsible for such operation.	Certification business rules and the records relating to the amendment thereof
4302	(b) Matters described in item 15(a) of Article 6 and the records relating to the amendment thereof (Article 12.1.3(b))	(2) The matters described in item 15(a) of Article 6 of the Ordinance (Operational Procedures) and the records related to the amendment thereof shall be prepared and preserved. The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Records relating to the amendment of operational procedures. Examples: * Administration guidelines and the regulations based thereon (including amendment records) * Document management regulations (including document architecture)
4303	(c) Matters described in item 15(b) of Article 6 and the records relating to the amendment thereof (Article 12.1.3(c))	(3) The matters described in item 15(b) of Article 6 of the Ordinance (responsibility and power of the person who engages in the operation and command structure) (including the organizational chart or system diagram related to personnel engaged in the certification business facility operation) and the records related to the amendment thereof shall be prepared and preserved. The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Records relating to operational responsibility Examples: * Organizational chart, including command structure * Amended records of the organizational chart, including command structure * Operational responsibility, authority regulations and amended records thereof * Records of the work order and order of removal
4304	(d) In the event the authentication operation is delegated in part to any other party, documents relating to consignment agreement (Article 12.1.3(d))	(4) In the event the authentication operation is delegated in part to any other party, the documents relating to the consignment agreement are prepared and preserved. The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Consignment agreement and supplemental memorandum

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
4305	(e) Records relating to the results of audit described in item 15(d) of Article 6	(5) The following records related to the results of an audit as described in item 15(d) of Article 6 of the Ordinance (matters relating to the operation audit) shall be prepared and preserved: ① Audit implementation records (including unscheduled audits) ② Audit report (relating to periodic audits) ③ Corrective measures report based on the results of audit The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Audit implementation records Examples: * Audit criteria and procedures * Matters to be audited and the details of audit * Questionnaire, etc. * Audit implementation records * Audit report * Security audit report * Corrective measures report
		4.4 Books and documents, etc. related to certification business facilities and security measures	
4401	The books and documents relating to the facilities and security measures as described below (Article 12.1.4) must be preserved from the date of preparation until the date of renewal of authentication (Article 12.3). Such books and documents (only those documents on which no signature or seal of the user or proxy is affixed) may be stored in electromagnetic recording media (Article 12.4). Those books and documents to be preserved must be the original thereof (except those documents provided in the preceding paragraph) (Article 12.5). (a) Records relating to the measures described in item 1 of Article 4 (except visual records) (Article 12.1.4(a))	(1) The following matters related to the measures described in item 1 of Article 4 of the Ordinance shall be recorded and the records shall be preserved. (Of the facilities used for the operation pertaining to the application, the computers and other systems/facilities used in the preparation/management of an electronic certificate shall be installed where the required measures have been implemented in accordance with the importance of the operations, for the purpose of managing access to/exit from the facility.) ① Date/hour and place of access to the room ② Information relating to the identification of the person who accesses to the room ③ Records relating to the operation of devices to access to the room ④ Records relating to the alarm	Records relating to the access to the room Examples: * Access control records for the certification facility room * Records relating to the alarm * Unauthorized personnel access records
4402	(b) Records relating to the measures described in item 2 of Article 4 (only those in the event of any unauthorized access) (Article 12.1.4(b))	(2) The following matters related to the measures described in item 2 of Article 4 of the Ordinance shall be recorded and the records shall be preserved. (All necessary measures shall be implemented in the certification business facility to prevent unauthorized access via telecommunications.) ① Of the firewall and intrusion detection system history, the records that show any abnormal condition (abnormal occurrence date and time, IP address of source computer, IP address of destination computer, communication protocol used, etc.)	Unauthorized access records Examples: * Firewall setting information and abnormal log * Abnormal log of intrusion detection system (e-mail information to the manager including the reasons for determining any abnormality * Security audit records
4403	(c) Records relating to the operation of certification business facilities described in item 3 of Article 4 (Article 12.1.4(c))	(3) The following matters related to the operation of a certification business facility as described in item 3 of Article 4 of the Ordinance shall be recorded and preserved. (All necessary measures shall be implemented in the certification business facility to prevent operation by any unauthorized person and such facilities must be able to record such operations.) ① Of the records relating to the operation of certification business facilities, the records related to the operation other than those related to the normal authentication operation and the records relating to any failure	Records relating to the operation of certification business facilities Examples: * Records relating to the abnormal operation and failure

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
4404	(d) Records relating to the permission described in item 16 of Article 6 (Article 12.1.4(d))	(4) The records related to the permission as described in Item 16, Article 6 of the Ordinance shall be prepared and the records shall be preserved. (The permission related to the access to the room where the certification business facilities are installed and the operation thereof as well as the management of identification codes relating to such permission shall be appropriately implemented in accordance with the importance of the operation conducted by such certification business facilities.) ① The foregoing records include the records regarding authorization management based on the regulations related to the permission by permission type. The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Permission records (including the person who determines to permit) Examples: * Books relating to the authorization (including information recording to biometrics device, password management records, etc.)
4405	(e) Records relating to the maintenance and management of certification business facilities and other facilities necessary for complying with the criteria described in each item of Article 4 (Article 12.1.4(e))	(5) The records relating to the maintenance and management of certification business facilities and other facilities necessary for complying with the criteria described in each item of Article 4 of the Ordinance are prepared and preserved. ① The records that include the records relating to the maintenance of facilities and the history relating to the modification of system. The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Maintenance records related to the certification business facilities Examples: * Maintenance records of certification business facilities* History of modification of certification business facilities * History of modification of certification business facilities * Records of transition to backup facilities * Records of maintenance and management of institution * Records of maintenance and management of certification facility room * Records of maintenance and management of certification facility room
4406	(f) Records relating to accident (Article 12.1.4(f))	(6) The records related to the accident shall be prepared and preserved. ① The foregoing records include records related to the unauthorized access of certification facility room, shutdown/unauthorized operation of a certification business facility, and the shutdown/unauthorized operation of devices used to manage access to the certification facility room (with the exception of historical records for firewall/intrusion detection systems indicating abnormal conditions), the reports related to the failure thereof (including the date/time failure occurred), and reports related to the restoration thereof. This includes the results related to restoration, (including the date/time of restoration and the name of the person who implemented the restoration.) The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Reports relating to the failure and restoration Examples: * Reports related to the failure of a certification business facility and the restoration thereof * Reports relating to the failure of access management device and the restoration thereof * Reports relating to the failure of registration terminal and the restoration thereof

Item	Implementation Ordinance	Conformity with Accreditation Criteria	Examples of Books and Documents
4407	(g) Records relating to the use and disposal of books and documents (Article 12.1.4(g))	(7) The records related to the use and disposal of books and documents shall be prepared and preserved. The foregoing records include any additional information relating to the date of implementation thereof, the identification of the person who implemented such operation, and the person who is responsible for such operation.	Records relating to the use and disposal of books and documents Examples: * Records related to the use and disposal of certification business rules, user agreements, signature verifier agreements, personal information protection regulations, and regulations based on administration guidelines