Accredited Certification Authority's Facilities and Equipment Assessment Criteria

[V1.0]

National Agency for Information and Communication Technologies

This document gives detailed evaluation items on facilities and equipment for setting up and running an Accredited Certification Authority (ACA). It also is aimed at auditing CAs' facilities and equipment.

< INDEX >

I . Overview

1. Purpose

Pursuant to the “Regulation of facilities and equipment of accredited certification authorities”, this document prescribes a check list of items with respective details of a digital signature-based certification system. These items are categorized as follows:

- Regulation of facilities and equipment of accredited certification authorities
- Protective facilities and equipment of a Certification Authority (CA);
- Certification system security and reliability;
- Encryption and digital signature functions;
- Certificate user registration information.

2. Definition

2.1 Terms used in these regulations are defined as follows:

1. "Digital signature creation key" means electronic data used for creating a digital signature.
2. "Digital signature verification key" means electronic data used for verifying a digital signature.
3. "Digital signature key" means a digital signature verification key which matches with a digital signature creation key.
4. "Accredited digital signature scheme" (hereinafter "certification scheme") means an architecture to provide

the issuance of certificates, the management of records related to certification services, additional practice using certificates and other related services.

5. "Accredited certification system" (hereinafter "certification system") means a system, supporting user registration information management; the creation and management of digital signature keys; the creation, issuance and management of certificates and time-stamping service, installed in a certification authority in order to carry out certification practice.
6. "Auditor" means a person who inquires and manages audit records of a certification system.
7. “Operator” means a person who is in charge of operating a certification system.
8. “Policy manager" means a person who establishes and manages policies relating to a certification system.
9.“Registration information" means information on user registration number, name, address, phone number, e-mail address, Distinguished Name(hereinafter "DN"), his/her certificate usage purpose and area.

3. Scope

These rules are applied to certification services using the asymmetric encryption-based digital signature technology.

Ⅱ. Check details

No.	Check item	Description
EI-01	Facilities to manage user registration information	1. It has a function to register and manage subscriber information included in his/her certificate. 2. It has a function to store subscriber certificate and others in a secure manner.
EI-02	Facilities to create and manage digital signature keys	1. It has a function to create and manage the digital signature key of an accredited certification authority. 2. It has a function to store the digital signature key securely.
EI-03	Facilities to create/issue/ manage certificates	1. It has a function to create/issue/store/notify a certificate. 2. Validity verification and auditing security functions are also pertained.
EI-04	Time-stamping facilities	1. A time-stamping function is pertained.
EI-05	Protective facilities	1. Facilities and equipment required to protect network and certification system that are providing certification services.
EI-06	User facilities	1. It has a function to manage user's digital signature key and certificate. 2. It has a function to verify the digital signature and certificate. 3. A time-stamping function is pertained. 4. It has a function to manage Software configuration.

※ The symbols and meanings used for audit item numbers and related basis are as follows.

- EI (Evaluation Items) : Evaluation items on carrying out an actual test
- RF (Regulation of Facility) : Regulation of facilities and equipment of accredited certification authorities

1. Facilities to manage user registration information

No.	Category	Check item	Description	Pursuant to
EI-01-01	Identifying Subscribers	Assigning DN in accordance with the certification system technical specifications 1.3	1. In case of new registration, It has a function to check the uniqueness of all of DN registered in the respective certification authority and a function to print out an error message with the same DN. 2. It has a function to confirm the uniqueness of the DN on reissuing and renewing of subscriber certificate. 3. It has a function to create a DN pursuant to Article 1.3 of the [Annex 2].	RF - 4.1.1
EI-01-02	Managing Subscribers' Registration Information	Entering, accessing, modifying and deleting registration information	1. It has a function to enter, store, modify, remove and search records such as registration date, registration category, subscriber name, resident registration number, DN, certificate usage, etc. 2. It has a function to print out an error message incase required information is not entered. 3. It has a function to figure out the lack of storage space needed to store user information. 4. It has a function to backup registration information periodically.	RF - 4.2.1
EI-01-03		Encryption and electronic signature of registration information transmitted over the network	1. It has a function to encrypt and digitally sign registration information with a secure cryptography or digital signature algorithm and then send the encrypted information. 2. It shall be confirmed whether there is a security procedure to create, store and distribute the encryption key and digital signature creation key of registration authority and proxy registration authority. 3. It shall be confirmed whether there is a procedure to send user registration information without using an information network. 4. It shall be confirmed whether there is a sender identification procedure in the event of not going through the information network.	RF - 4.2.2

No.	Category	Check item	Description	Pursuant to
EI-01-04	Audit and Security	Generating and storing audit records concerning details on how, when and by whom entry, access, change and deletion of registration information	1. It has a function to store audits of respective record identifier, case type, date and time. 2. It has a function to search audit records	RF - 4.3.1 A
EI-01-05		Backing up audit records	1. It has a function to backup audit records periodically	RF - 4.3.1 B
EI-01-06		Coping with such threats as forgery, alteration and deletion of audit records	1. It has a function to protect against audit records modification. 2. It has a function to detect alteration by digitally signing or hashing audit records. 3. It has a function to figure out the lack of storage space for audit records.	RF - 4.3.2 A
EI-01-07		Coping with threats such as forgery, alteration and deletion of the information registration management software	1. It has a protection function not to alter or remove software. 2. It has a function to detect alteration by digitally signing or hashing audit records.	RF - 4.3.2 B
EI-01-08		Differentiating the roles of the operation manager and the audit manager with regards to access control	1. It has functions to set authorities for operators and auditors with regard to access control. 2. In the event of using a password, it has a function to keep the password securely stored in a system with encryption and hashing.	RF - 4.3.2 C (1)

No.	Category	Check item	Description	Pursuant to
EI-01-08		Classifying the roles of other managers, if any, with regard to access control	1. In case, there is more than one administrator, it has a function to set authorities of each administrator with regard to access control 2. In the event of using a password, it has a function to keep the password securely stored in a system with encryption and hashing.	RF - 4.3.3 C(2)
EI-01-09		Classifying the roles of other managers, if any, with regard to access control	1. In the event there is more than one administrator, it has a function to set authorities for the administrator with regard to access control. 2. In the event of using a password, it has a function to keep the password securely stored in a system with encryption and hashing.	RF - 4.3.3 C(2)
EI-01-10		Coping with threats such as forgery, alteration, deletion and leakage of registration information	1. It has a function to detect alteration by hashing or digitally signing registration information.	RF - 4.3.3 D
EI-01-11	Managing the Configuration of Registration Information Management Software	Configuration management of software managing registration information	1. It has a function to manage the configuration of information registration management software by hashing. 2. It shall be confirmed whether there is a procedure for the configuration management of the software managing registration information	RF - 4.4

No.	Category	Check item	Description	Pursuant to
EI-01-12	Equipment for Storing Subscribers' Registration Information	Certification authorities must have a cabinet or safe for storing subscribers' registration information with a locking mechanism in a place separated from the office area in certification authorities.	1. It has a function to store subscriber's certificate related information in a repository with a specific access control device. 2. It shall be confirmed whether intrusion detection equipment such as CCTV, camera, etc. in the repository has been installed. 3. It shall be confirmed whether subscriber information is stored in a cabinet or secure box with a lock.	RF - 4.5

2. Facilities to create and manage digital signature keys

No.	Category	Check item		Description	Pursuant to
EI-02-01	Algorithm	Accredited system	Generating and validating RSA digital signature	1. In case of using a RSA digital signature algorithm, it shall have a function to create/verify a digital signature according to PKCS #1.	RF - 2.1.1 A (1)(A)
EI-02-02			Generating and validating ECDSA electronic signature	1. In case of using an ECDSA digital signature, it shall have a function to create/verify a digital signature according to ANSI X9.62.	RF - 5.1.1 A (1)(B)
EI-02-03		Subscriber equipment	Generating and validating RSA digital signature	1. In case of using of a RSA digital signature algorithm, it has a function to create/verify a digital signature according to PKCS #1.	RF - 5.1.1 A (2)(A)
EI-02-04			Generating and validating ECDSA electronic signature	1. In case of using an ECDSA digital signature algorithm, it has a function to create/verify a digital signature according to ANSI X9.62.	RF - 5.1.1 A (2)(B)
EI-02-05	Algorithm	Accredited system	Generating RSA 2048 bit or longer key pairs	1. It has a function to create a RSA 2048-bit or longer digital signature key. 2. In case of RSA, it has a function to create random number, decimal and digital signature key according to ANSI X9.31. 3. In case of using a pseudo-random creation device, it has a function to meet a FIPS 140-1 random statistic test.	RF - 5.1.1 B (1)(A)

No.	Category	Check item		Description	Pursuant to
EI-02-06			Generation of ECDSA 160bit or longer key pairs	1. It has a function to create an ECDSA 160-bit or longer digital signature key. 2. In case of using ECDSA, it has a function to use a domain parameter (curve parameter) pursuant to "digital signature standard" among certification scheme's technical standards. 3. In case of using ECDSA, it has a function to create random number, decimal and digital signature key.	RF - 5.1.1 B (1)(B)
EI-02-07			Generating RSA 2048 bit or longer key pairs	1. It has a function to create a RSA 2048-bit or longer digital signature key. 2. In case of RSA, it has a function to create random number, decimal and digital signature pursuant to ANSI X9.31. 3. In case of using a pseudo-random creation device, it has a function to meet a FIPS 140-1 random statistic test.	RF - 5.1.1 B (2)(A)
EI-02-08	Algorithm	Subscriber equipment	Generation of ECDSA 160bit or longer key pairs	1. It has a function to create an ECDSA 256-bit or more longer digital signature key ECDSA. 2. In the event of ECDSA, it has a function to use a domain parameter (curve parameter) pursuant to "digital signature standard" among certification scheme's technical standards. 3. In the event of ECDSA, it has a function to create random number, decimal and digital signature key pursuant to ANSI X9.62.	RF - 5.1.1 B (2)(A)
EI-02-09		Accredited system	Generating SHA-256bit or longer hash values	1. In case of SHA-256, it has a function to comply with FIPS 180-1 on creating a hash value. 2. It has a function to create a longer than 256-bit hash value.	RF - 5.1.2 A(1)
EI-02-10		Subscriber equipment	Generating SHA-256 bit or longer hash values	1. In case of SHA-256, it has a function to comply with FIPS 180-1 on creating a hash value. 2. It has a function to create a hash value longer than 256-bit.	RF - 5.1.2 B(1)

No.	Category	Check item		Description	Pursuant to
EI-02-11		Encryption and decryption by means of the cryptographic algorithm specified in certification system technical specifications 2.3		1. In case of SEED, it has a function to comply with TTAS.KO-12.0004 on conducting encryption. 2. In case of 3-DES, it has a function to comply with FIPS 46-3 on conducting encryption.	RF - 5.1.3 A
EI-02-12	Equipment for Generating and Managing Certification Authorities' Key Pairs	Setting and verifying information on the generation of key pairs like the type of algorithm, the length of the key, and its use		1. It has a function to set and confirm algorithm, key length, key creation information on usage that are presented by "digital signature algorithm standard". 2. It has a function to create a key which is only based on information that has been set.	RF - 5.2.1 A(1)
EI-02-13		Confirming whether it meets with article 6.4 of the [Annex 2, certification scheme's technical standards]	In case of receiving FIPS 140-1 Level 3 from NIST	1. It shall be confirmed whether there is the FIPS 140-1 Level 3 certificate which has been submitted.	RF - 5.2.2 A
EI-02-13		Confirming whether it is to meet article 6.4 of the [Annex 2, certification scheme's technical standards]	In case of not receiving FIPS 140-1 Level 3 from NIST`	1. It has a function to keep digital signature key and encryption key securely in an encryption module. 2. It shall be confirmed whether a pseudo-random creation device is used for creating a pseudo-random number and has passed "Monobit, Poker, Run, Long Run tests". 3. It has a function to create a key with the procedure which ensures security. 4. It has a function to input/output a key in a secure manner. 5. It has a function to deny access to digital signature key and encryption key stored by unauthenticated persons. 6. It has a function to initialize all digital signature keys and encryption keys to NULL while destroying the keys.	RF - 5.2.2 A

No.	Category	Check item	Description	Pursuant to
EI-02-14		Generating key pairs by means of the electronic signature algorithm specified in 5.1.1	1. It has a function to create a digital signature by using an algorithm presented in "digital signature algorithm standard"(certificate scheme's technical standards).	RF - 5.2.3 A
EI-02-15		Generating and storing audit record details of key pair generation and electronic signatures	1. It has a function to store audits for respective record identifier, case type, date and time and others. 2. It has a function to search the audit records.	RF - 5.2.4 A
EI-02-16		Backing up Audit Records	1. It has a function to backup audit records periodically.	RF - 5.2.4 B
EI-02-17		Coping with threats such as the forgery, alteration and deletion of audit records	1. It has a function to protect against audit records alteration. 2. It has a function to detect alteration by hashing or digitally signing the audit records. 3. It has a function to figure out the lack of storage space for audit records.	RF - 5.2.4 B(1)
EI-02-18		Coping with threats such as the forgery, alteration and deletion of the key pair generation and management software	1. It has a function to protect against software alteration or deletion. 2. It has a function to detect alteration by hashing or digitally signing software.	RF - 5.2.4 B(2)
EI-02-19		Differentiating the roles of the operation manager and the audit manager with regard to control access	1. It has a function to set authorities for operators and auditors in order to conduct access control. 2. In case of using a password, it has a function to securely store the password in a system with encryption and hashing.	RF - 5.2.4 B (3)(A)
EI-02-20		Differentiating the roles of other managers, if any with regard to control access	1. In case there is more than one administrator, it has a function to set authorities for each administrator in order to control access. 2. In case of using a password, it has a function to securely store the password into a system with encryption and hashing.	RF - 5.2.4 C (3)(B)

No.	Category	Check item	Description	Pursuant to
EI-02-21	Facilities to create and manage the digital signature key of an accredited certification authority	Three or more authorized employees jointly generate and manage key pairs by means of access control functions like passwords, hardware tokens and biometrics	1. As an access control function such as password, hardware token and biometrics, it has a function to create and manage a digital signature key by 3 or more authorized persons.	RF - 5.2.5
EI-02-22		Managing the configuration of the certification authority key pair generation and management software	1. It has a function to manage the configuration of software creating and managing a digital signature key.	RF - 5.2.6
EI-02-23		Redundancy of the equipment for generating and managing certification authority key pairs	1. It has a duplicate of the facilities managing the digital signature keys of accredited certification authorities.	RF - 5.2.7

※ In the event of using a HSM device for the functions of EI-02-25, EI-02-26 or EI-02-27, you must comply with EI-02-13.

3. Facilities to create/issue/manage certificates

No.	Category	Check item	Description	Pursuant to
EI-03-01	Generating and Issuing Certificates	Processing certification system technical specifications 3.1	1. It has a function to carry out pursuant to the wired/wireless CSR (Certificate signing request) of a digital signature certification management scheme. 2. It has a function to create a response message for the wired/wireless CSR. 3. It has a function to support DER or Base64 as a coding format on creating the response message.	RF - 6.1.1 A(1) RFC 2511
EI-03-02		Verifying that the private key belongs to the subscriber	1. It has a function to confirm a digital signature creation key is pertained to owner (subscriber).	RF - 6.1.1 A(2)
EI-03-03		Examining the uniqueness of the subscriber's public key	1. It has a function to confirm the uniqueness of a subscriber's digital signature verification key. 2. In case of re-issuance or renewal, it has a function to check the uniqueness.	RF - 6.1.1 A(3)
EI-03-04		In case certificate request is made over a network, Handling a certificate issuing request in accordance with certification system technical specifications 3.2	1. It has a function to carry out according to a wired/wireless certificate management protocol (certification scheme's technical standards). 2. It has a function to create a response message for the wired/wireless certificate management protocol. 3. It has a function to support DER or Base64 as a coding format on creating the response message.	RF - 6.1.1 A(4)
EI-03-05		Establishing the certificate generation policy	1. It has a function to set policies for digital signature algorithm, certificate's valid period, usage scope and certificate's extension fields.	RF - 6.1.1 B
EI-03-06		Performing access control separately by differentiating the certificate generation from the certificate generation policy formulation and appointing managers	1. It has a function to perform access control for each administrator with respect to his/her role. 2. In case of using a password by an authorized person, it has a function to securely safe the password with encryption and hashing.	RF - 6.1.1 C

No.	Category	Check item	Description	Pursuant to
EI-03-07		Generating certificates in accordance with generation policies	1. It has a function to create a certificate pursuant to the certificate creation policy that has been set.	RF - 6.1.1 D(1)
EI-03-08		Generating certificates with the electronic signature function of the key pair generation and management equipment (5.1.1)	1. It has a function to create a certificate by using a digital signature function to create/manage/facilitate a digital signature key (5.1.1). 2. It has a function to remove the digital signature creation key from a memory or temporary file after signing is completed. 3. It has a function to carry out the integrity check of the digital signature creation key. 4. It has a function to distinguish or identify two or more authorized persons. 5. It has a function to protect the digital signature creation key pursuant to Rule 6.4 of the [Annex 2, certification scheme's technical standards].	RF - 6.1.1 D(2)
EI-03-09		Generating certificates in accordance with certification system technical specifications 1.1	1. It has a function to create a certificate pursuant to rule 1.1 of the [Annex 2] among certification scheme's technical standards. 2. It has a function to support DER as a coding format on creating a certificate by using public key information. 3. It has a function to give the unique serial number of the certificate. 4. It has a function to delete all information used to create a pseudo-random number after the number has been stored into a medium. 5. The content, format and location of identification information that will be stored in a certificate must be pursuant to technical standards.	RF - 6.1.1 D(3)
EI-03-10		Querying certificate's related information	1. It has a function to inquiry digital signature algorithm, certificate validity, subscriber and issuer DN, usage scope, extension fields, suspension/revocation, etc.	RF - 6.1.1 E

No.	Category	Check item	Description	Pursuant to
EI-03-11		Recording information related to suspension, restoration, revocation, request date and others	1. It has a function to record suspension/recovery/revocation, request date, reason and other matters.	RF - 6.1.2 A(1)
EI-03-12		Checking if the status of the certificate is appropriate for processing of requests	1. It has a function to confirm whether the status of a respective certificate is adequate enough to process a request.	RF - 6.1.2 A(2)
EI-03-13		In case request is made or handled over a network, handling a request for certificate suspension and revocation in accordance with certification system technical specifications 3.2	1. It has a function to carry out suspension or revocation of a certificate through an information network pursuant to rule 3.2 [Annex 2, certification scheme's technical standards].	RF - 6.1.2 A(3)
EI-03-14		In case a request for certificate suspension and revocation is made over the network, the Electronic signature of the received and transmitted information	1. It has a function to digitally sign information sent or received on requesting or carrying out the certificate suspension or revocation through the information network.	RF - 6.1.2 A(4)
EI-03-15		Establishing certificate suspension and revocation list and generation policies	1. It has a function to set digital signature algorithm, next issuance date, CRL (certificate revocation list), CSL (certificate suspension list), extension fields and auto-renewal/alarm prior to the next issuance date.	RF - 6.1.2 B

No.	Category	Check item	Description	Pursuant to
EI-03-16		Performing access control by differentiating the certificate generation function from the certificate generation policy formulation function and appointing managers	1. It has a function to control access for each administrator of different categories and roles. 2. In case of using a password by authorized persons, it has a function to securely safe the password with encryption and hashing.	RF - 6.1.2 C
EI-03-17		Generating certificate suspension and revocation lists with the Electronic signature functions of the equipment for generating and managing key pairs (5.1.1)	1. It has a function to create and manage a CRL or CSL by using a function (5.1.1) to digitally sign facilities for creation and management of a digital signature key. 2. It has a function to remove a digital signature creation key from a memory or temporary file as soon as the signing is completed. 3. It has a function to assign the unique serial number of the certificate. 4. It has a function to delete all information used to create a pseudo-random number after the number has been stored in a medium. 5. The content, format and location of identification information that will be stored in a certificate must be pursuant to technical standards.	RF - 6.1.2 D(1)
EI-03-18	Facilities to create and issue certificates	Generating certificate suspension and revocation lists in accordance with the generation policy conforming to certification system technical specifications 1.2 for certificate suspension and revocation list profile	1. It has a function to create CRL or CSL pursuant to the policy that has been set. 2. It has a function to associate suspension to a reason code value. 3. It has a function to automatically input the correct current time as suspension or revocation date. 4. It has a function to support DER as a coding format on creating a CRL or CSL.	RF - 6.1.2 D(2)
EI-03-19		Querying certificate information on suspension and revocation lists	1. It has a function to inquire digital signature algorithm, issuance date, next issuance date, serial number of a certificate suspended or revoked, suspension or revocation date, reason and extension fields of CRL and CSL.	RF - 6.1.2 E

No.	Category	Check item	Description	Pursuant to
			2. It has a function to record respective certificate information on the CRL or CSL.	
EI-03-20		Revoking certificates 6 months after suspension	1. It has a function to revoke a certificate after 6 months from the day when the certificate was suspended.	RF - 6.1.2 F
EI-03-21		Equipment to store subscribers' certificates and the records on their respective suspension and revocation for a period of 10 years after their expiration	1. It has a facility to store a subscriber's certificate and the records of its suspension or revocation for 10 years from the day when the respective certificate has expired, according to the regulation in force.	RF - 6.1.3 A
EI-03-22		Remote storage equipment at least 10km away from that storing subscribers' certificates and the records of their suspension and revocation	1. It is remote storage equipment at least 10km away from that storing subscriber certificates and the records of their suspension and revocation. 2. It is required to build a backup Center for storage of subscribers' certificates and records of their suspension and revocation	RF - 6.1.3 B(1)
EI-03-23		Physical access control devices and locking mechanism like HSM, smartcard, biometrical device for remote storage equipment	1. They are physical access control devices and locking mechanism like HSM, smartcard, biometrical device for remote storage equipment	RF - 6.1.3 B(2)
EI-03-24		Collecting and storing audit records of accesses to remote storage equipment	1. It has a function to Collect and store audit records of accesses to remote storage equipment.	RF - 6.1.3 B(3)
EI-03-25		Intrusion monitoring devices for remote storage equipment	1. It is an intrusion monitoring device for remote storage equipment or CCTV.	RF - 6.1.3 B(4)
EI-03-26		Generating and storing the	1. It has a function to generate and store the details of certificate issuance,	RF - 6.1.4

No.	Category	Check item	Description	Pursuant to
		details of certificate issuance, suspension, restoration, revocation and policy formulation	suspension, restoration, revocation, and policy formulation. 2. It has a function to search audit records.	A(1)
EI-03-27		Backing up audit records	1. It has a function to back up audit records	RF - 6.1.4 A(2)
EI-03-28		Coping with threats such as forgery, alteration and deletion of audit records	1. It has a function to protect against audit records alteration. 2. It has a function to detect alteration by hashing or digitally signing audit records. 3. It has a function to figure out the lack of storage space for audit records.	RF - 6.1.4 B(1)
EI-03-30		Coping with threats such as forgery, alteration and deletion of the certificate generation and issuance software	1. It has a function protect against software alteration and deletion. 2. It has a function to detect alteration by hashing or digitally signing software.	RF - 6.1.4 B(2)
EI-03-31		Differentiating the roles of each manager with regards to access control	1. If there are two or more administrators, it has a function to set authorities for each of the administrator with regard to access control. 2. In the event of using a password, it has a function to securely safe the password in a system with encryption and hashing	RF - 6.1.4 B (3)(B)
EI-03-32		Managing configuration of the Certificate Generation and Issuance Software	1. It has a function to manage the configuration of software creating and managing certificate by hashing. 2. It shall be confirmed whether there is a procedure for configuration management of software creating and issuing certificates.	RF - 6.1.5
EI-03-33		Redundancy of certificate generation and issuance equipment	1. It has a duplicate of certificate generation and management system.	RF - 6.1.6 A

No.	Category	Check item	Description	Pursuant to
EI-03-34		Emergency recovery through certificate generation and issuance equipment redundancy	1. It has a function to carry out emergency recovery by using duplicate of certificate generation and issuance devices.	RF - 6.1.6 B
EI-03-35	Facilities to notify certificates and to confirm their validity	Registering and deleting certificate, certificate suspension and revocation lists	1. It has a function to register and delete certificate, certificate suspension and revocation lists by using DN. 2. Regarding Cameroonian directories and web servers, it has a function to support Cameroonian DN values and UTF8 String type coding.	RF - 6.2.1 A
EI-03-36		Searching certificate, certificate suspension and revocation lists in accordance with certification system technical specifications 4.1	1. It has a function to search subscriber certificates, etc. through DN pursuant to a directory-related protocol (certification scheme's technical standards). 2. It has a function to search subscriber certificate, etc. through LDAP, HTTP or OCSP interfaces.	RF - 6.2.1 B
EI-03-37		Generating audit records of certificate, certificate suspension and revocation lists while taking note of the time it occurred, and the person who carried out the operation	1. It has a function to securely register the audit records of a directory or web server regarding information on respective record, case type, checking succeeded or failed, date and time and someone who behaves. 2. It has a function to search the audit records.	RF - 6.2.1 C (1)(A)
EI-03-38		Backing up audit records	1. It has a function to back up audit records.	RF - 6.2.1 B (1) (B)
EI-03-39		Coping with threats such as forgery, alteration and deletion of audit records	1. It has a function to protect against audit records alteration. 2. It has a function to detect alteration by hashing or digitally signing audit records. 3. It has a function to figure out the lack of storage space for audit records.	RF - 6.2.1 C (1)(A)

No.	Category	Check item	Description	Pursuant to
EI-03-40		Coping with threats such as forgery, alteration and deletion of notification software for certificate suspension and revocation list	1. It has a function to protect against software alteration or deletion. 2. It has a function to detect alteration by hashing or digitally signing software.	RF - 6.2.1 C (2)(B)
EI-03-41		Differentiating the roles of the operation manager and the audit with regard to access control	1. It has a function to set authorities for operators, auditors, etc. and to do access control. 2. In case of using a password, it has a function to securely save the password in a system through encryption and hashing.	RF - 6.2.1 C (2) (B) 1)
EI-03-42		Differentiating the roles of managers with regard to access control	1. If there are two or more administrators, it has a function to set authorities for each of them with regards to access control. 2. In case of using a password, it has a function to securely keep the password (through encryption and hashing).	RF - 6.2.1 C (2)(C) 2)
EI-03-43		Coping with threats such as forgery, alteration and deletion of certificate, certificate suspension and revocation lists	1. It has a function to cope with threats such as the forgery, alteration and deletion of certificate, certificate suspension and revocation lists.	RF - 6.2.1 C (2)(D)
EI-03-44		Redundancy of certificate, certificate suspension and revocation list notification equipment	1. It has a duplicate certificate, certificate suspension and revocation list notification equipment	RF - 6.2.1 D(1)
EI-03-45		Real-time emergency recovery function by means of redundant certificate, certificate suspension and revocation lists notification equipment	1. It has a function to carry out real-time emergency recovery function with redundant certificate, certificate suspension and revocation lists.	RF - 6.2.1 D(2)

4. Time-stamping facilities

No.	Category	Check item	Description	Pursuant to
EI-04-01	Time receiving	Receiving the current time pursuant to rule 4.3 of the [Annex 2, certification scheme's technical standards]	t has a function to receive the current time pursuant to rule 4.3 of the [Annex 2, certification scheme's technical standards].	RF - 7.1.1 A
EI-04-02		Expressing 1/1000 second	t has a function to express 1/1000 second.	RF - 7.1.1 B
EI-04-03		Notifying an administrator when a problem occurs on a time-receiving device	t has a function to alert an administrator when a problem occurs on the time-receiving device.	RF - 7.1.1 C
EI-04-05		Starting a time-stamping service on modifying the correct time regarding the time of time-checking system	1. It has a function to start a time-stamping service on modifying the correct time regarding the time of a time-checking system.	RF - 7.1.2 A(1)
EI-04-06		Supporting a time-modifying function continually.	1. It has a function to support a time-modifying function continually.	RF - 7.1.2 A(2)
EI-04-07		In case of malfunctioning of time-modifying function and suspending a time-stamping service, print out an error message	1. It has a function to print out an error message for an error occurred on a time-modifying function and suspending a time-stamping service.	RF - 7.1.2 B(2)
EI-04-08	Time checking service	Providing a time-stamping service pursuant to rule 4.2 of the [Annex 2, certification scheme's technical standards]	1. It has a function to provide a time-stamping service pursuant to rule 4.2 of the [Annex 2, certification scheme's technical standards].	RF - 7.2.1 A

No.	Category	Check item	Description	Pursuant to
EI-04-09	Time stamping service	Providing a time-stamping service by using an algorithm (prescribed in article 1 of paragraph 1 of provision 5)	1. It has a function to provide a time-stamping service by using an algorithm (prescribed in article 1 of paragraph 1 of provision 5.)	RF - 7.2.1 B
EI-04-10		Checking whether time recorded on a time-stamping token received by a user matches with issuance record time	1. It has a function to check whether time recorded on a time-stamping token received by a user matches with issuance record time.	RF - 7.2.1 C
EI-04-11		Providing a time-stamping service with the function to digitally sign facilities creating and managing a digital signature key	1. It has a function to provide a time-stamping service by using the function to digitally sign facilities creating and managing a digital signature key.	RF - 7.2.1 D
EI-04-12		Creating, storing and backing up audit records	1. It has a function to create, store and back up audit records such as time-modifying details, time-stamping fact, time, requester, problem occurred and the time, delaying in providing time-stamping service. 2. It has a function to search audit records. 3. It has a function to back up audit records.	RF - 7.2.2 A
EI-04-13		Coping with threats such as forgery, alteration and deletion of audit records	1. It has a function to protect against audit records alteration. 2. It has a function to detect alteration by hashing or digitally signing audit records. 3. It has a function to figure out the lack of storage space for audit records.	RF - 7.2.2 B (1)(A)
EI-04-14		Coping with threats such as forgery, alteration and deletion of time-stamping software	1. It has a function to protect against software alteration. 2. It has a function to detect alteration by hashing or digitally signing software.	RF - 7.2.2 B (1)(B)

No.	Category	Check item	Description	Pursuant to
EI-04-15		Setting authorities for operators and auditors with regard to access control	1. It has a function to set authorities for operators, auditors and others with regards to access control. 2. In case of using a password, it has a function to securely store the password in a system through encryption and hashing.	RF - 7.2.2 B (1)(C) 1)
EI-04-16		In case there are two or more administrators, setting authorities for each of them with regard to access control	1. In case there are two or more administrators, it has a function to set authorities for each of them with regard to access control. 2. In case using a password, it has a function to securely store the password in a system through encryption and hashing.	RF - 7.2.2 B (1)(C) 2)
EI-04-17		Configuration management of time-stamping software	1. It has a function to manage the configuration of registration information-management software with version and hashing. 2. It shall be confirmed whether there is a procedure for configuration of registration information-management software.	RF - 7.2.2 C
EI-04-18		Are there redundancies for validity-checking facilities?	1. It shall be confirmed that validity-checking have redundancies.	RF - 7.2.2 D(1)
EI-04-19		Does it have a real-time recovery function at emergency by duplicating certificate validity-checking facilities?	1. It has a function to carry out a real-time recovery function at emergency by applying redundancies on certificate validity-checking facilities.	RF - 7.2.2 D(2)

5. Protective facilities

No.	Category	Check item	Description	Pursuant to
EI-05-01	Network and system security facilities	Using two or more network lines (Accesses to Internet) that are physically separated	1. It has a function to use two or more network lines (Accesses to Internet) that are physically separated.	RF - 8.1.1 A (1)(A)
EI-05-02		Using a line (Access to Internet) from two or more separate ISP (or IX)	1. It has a function to use a line (Access to Internet) from two or more separate ISP (or IX)	RF - 8.1.1 A (1)(B)
EI-05-03		Providing certification services continually even if failure occurs on a line (Access to Internet)	1. It has a function to provide certification services continually even if a failure occurs on a line (Access to Internet)	RF - 8.1.1 A (1)(C)
EI-05-04		Using a network line(Access to Internet) as a dedicated line for certification practice	1. It has a function to use a network line as a dedicated line for certification practice	RF - 8.1.1 A (1)(D)
EI-05-05		Providing certification services continually even if a failure occurs on a line	1. It has a function to provide two or more paths as an internal network. 2. It has a function to provide certification services continually even if a failure occurs on a path.	RF - 8.1.1 A (2)(A)
EI-05-06		Applying redundancies on routers	1. It has a function to use the redundancy of routers. 2. It has a function to use a router supporting a packet-filtering method.	RF - 8.1.1 A (2)(B)
EI-05-07		Redundancy of an intrusion prevention system	1. It has a function to apply redundancies on the intrusion prevention system.	RF - 8.1.1 B (1)(A)
EI-05-08		Using intrusion prevention software with CC grade or higher	1. It has a function to operate a duplicated intrusion prevention system with CC grade or higher.	RF - 8.1.1 B (1)(B)
EI-05-09		Setting access control regulations required for certification scheme	1. It has access control regulations required for certification practice.	RF - 8.1.1 B (1)(C)

No.	Category	Check item	Description	Pursuant to
EI-05-10		Storing and backing up records that an intrusion prevention system processes	1. It has a function to store and back up records that an intrusion prevention system processes.	RF - 8.1.1 B (1)(D)
EI-05-11		Using intrusion detection software with CC grade or higher	1. It has an intrusion detection software with CC grade or higher.	RF - 8.1.1 B (2)(A)
EI-05-12		Checking all traffic and detecting intrusion	1. It has a function to check all traffic and to detect intrusion.	RF - 8.1.1 B (2)(B)
EI-05-13		Continually providing pattern updates against new intrusion	1. It has a function to continually provide pattern updates against new intrusion.	RF - 8.1.1 B (2)(C)
EI-05-14		Informing an administrator of intrusion detected	1. It has a function to inform an administrator of intrusion detected.	RF - 8.1.1 B (2)(D)
EI-05-15		Systems or devices which are able to check the status of a network or system on real-time	1. It has a function to operate systems or devices which are able to check the status of a network or system on real-time. 2. It has a function to send SMS after alarms are set.	RF - 8.1.1 C(1)
EI-05-16		Systems or devices which are able to monitor programs or working processes of a certification system	1. It has operation systems or devices which are able to monitor programs or working processes of a certification system.	RF - 8.1.1 C(2)
EI-05-17		Access control for network devices such as switch, router, etc.	1. It has a function to prepare and operate the management policy for other devices (switches, routers, firewalls, etc) that are being operated related to certification practice.	RF - 8.1.1 D(1)
EI-05-18		Details of access control, settings and preventive measures built on network equipment	1. It has a function to record and store details of access control, settings and preventive measures built on network equipment.	RF - 8.1.1 D (2)(A)

No.	Category	Check item	Description	Pursuant to
EI-05-19		Setting accounts for each administrator related to access control with smartcard, biometric	1. It has a function to set separate accounts of each administrator related to access control with smartcard, biometric, etc	RF - 8.1.2 A(1)
EI-05-20		User registration required to accredited certification practice	1. It has a duty to facilitate user registration process	RF - 8.1.2 A(2)
EI-05-21		Installing only software needed for the system operation	1. It has a duty to only install and operate software needed for accredited certification practice.	RF - 8.1.2 A(3)
EI-05-22		Running only programs or processes tailored for the purpose of system operation	1. It has a duty to run only programs or processes tailored for accredited certification practice.	RF - 8.1.2 A(4)
EI-05-23		Carrying out maintenance program	1. It has a duty to conduct maintenance program.	RF - 8.1.2 A(5)
EI-05-24		Conducting OS patches	1. It has a duty to carry out OS patches.	RF - 8.1.2 A(6)
EI-05-25		Checking whether a maintenance contract regarding system and related software is made	1. It shall be confirmed whether a maintenance contract regarding system and related software is made.	RF - 8.1.2 A(7)
EI-05-26		System start-up /suspension	1. It has a function to create and store audit records for system start-up/suspension.	RF - 8.1.2 B(1)
EI-05-27		Start-up/termination of a program necessary for accredited certification practice	1. It has a function to create and store audit records for start-up/termination of a program necessary for accredited certification practice.	RF - 8.1.2 B(2)
EI-05-28		Log-in/log-out of root and users	1. It has a function to create and store audit records for log-in/log-out of root and users.	RF - 8.1.2 B(3)

No.	Category	Check item	Description	Pursuant to
EI-05-29		Complying with 8.1.2 A and 8.1.2 B regarding web server, name server, mail server, etc. necessary for certification practice	1. It has a function to comply with 8.1.2 A and 8.1.2 B regarding web server, name server, mail server, etc. necessary for certification practice.	RF - 8.1.2 C(1)
EI-05-30		Facilities providing a function to manage subscriber registration information, management of the digital signature key of an accredited certification authority and facilities providing a function to create and issue certificates may be installed in the same operation room but they must be separated from other facilities	1. It shall be confirmed whether facilities providing a function to manage subscriber registration information, management of the digital signature key of an accredited certification authority and facilities providing a function to create and issue certificates may be installed in the same operation room but they must be separated from other facilities.	RF - 8.2.1 A (1)(A)
EI-05-31	Physical security facilities	Facilities providing certificate notification must be separate from other facilities	1. It shall be confirmed whether facilities providing certificate notification must be separated from other facilities in a special operation room.	RF - 8.2.1 A (1)(B)
EI-05-32		Facilities providing certificate-status checking and time-stamping may be installed in the same operation room but they must be separated from other facilities	1. It shall be confirmed whether facilities providing certificate-status checking and time-stamping may be installed in the same operation room but they must be separated from other facilities.	RF - 8.2.1 A (1)(C)
EI-05-33		Building outer walls with bricks, reinforced concrete and welded	1. It shall be confirmed that outer walls are built with bricks, reinforced concrete and an iron frame which is welded with a 3T or heavier iron plate.	RF - 8.2.1 A (2)(A)
EI-05-34		Furnishing outer walls from the ceiling to the floor	1. It shall be confirmed whether outer walls are furnished from the ceiling to the floor.	RF - 8.2.1 A (2)(B)

No.	Category	Check item		Description	Pursuant to
EI-05-35		Building inner walls and the hall of the operation room of a certification system with bricks and frame of heavier iron plate		1. It shall be confirmed whether inner walls and the hall of the operation room of a certification system is constructed with bricks and an iron frame which is welded with an 1.8T and heavier iron plate.	RF - 8.2.1 A (3)(A)
EI-05-36		Furnishing of inner walls from the ceiling to the floor		1. It shall be confirmed whether inner walls are perfectly furnished from the ceiling to the floor	RF - 8.2.1 A (3)(B)
EI-05-37		Physical access control of the entrance gate of the operation room of a certification system	In case of a general door, enforcement and fire prevention functions	1. It shall be confirmed whether it has enforcement and fire prevention functions in case of a general door.	RF - 8.2.1 A (4)(B)
EI-05-38		Physical access control of the entrance gate of the operation room of a certification system	In case of a general door, enforcement and fire preventive measures	1. It shall be confirmed whether it has enforcement and fire preventive measures in case of a general door.	RF - 8.2.1 A (4)(B)
EI-05-39		Using windows with coated glass, tempered glass or tempered film		1. It shall be confirmed whether windows used are of coated glass with tempered glass or tempered film.	RF - 8.2.1 B (1)(A)
EI-05-40		Removing the lumber support of windows		1. It shall be confirmed whether the lumber support of windows is removed.	RF - 8.2.1 B (1)(B)
EI-05-41		Coating processing to prevent seeing inside		1. It shall be confirmed whether coating process to prevent seeing inside through windows is done.	RF - 8.2.1 B (1)(C)

No.	Category	Check item	Description	Pursuant to
EI-05-42		In case people can see through a ventilating window, installing a blackout curtain	1. It shall be confirmed whether a blackout curtain is installed if people can see through a ventilating window.	RF - 8.2.1 B (2)(A)
EI-05-43		Physical access control in order not to access the operation room of a certification system by unauthenticated persons	1. It has a function to carry out physical access control in order not to access the operation room of a certification system by unauthenticated persons.	RF - 8.2.2 A(1)
EI-05-44		Audit records of access control devices	1. It has a function to record audit information of access control devices such as serial number, case type, succeeded or failed checking, failure reason, date and time and others.	RF - 8.2.2 A(2)
EI-05-45		Biometric-based identification (fingerprint, iris, etc.)	1. It has a function to use access control devices with biometric-based identification (fingerprint, iris, etc.)	RF - 8.2.2 B(1)
EI-05-46		Possession-based identification (key, card, etc.)	1. It has a function to use access control devices with possession-based identification (key, card, etc.)	RF - 8.2.2 B(2)
EI-05-47		Facilities to prevent against invasion to the operation room of a certification system by unauthorized persons	1. It shall be confirmed whether facilities to prevent against invasion to the operation room of a certification system by unauthorized persons are installed.	RF - 8.2.2 C
EI-05-48		Able to record audits and conduct access control even if the electricity fails	1. It has a function to record audits and conduct access control even if electricity fails.	RF - 8.2.2 D
EI-05-49		Installing vibration detection device, sound detection device, intrusion detection device, etc inside an operation room	1. It shall be confirmed whether vibration detection device, sound detection device, intrusion detection device, etc are installed inside an operation room.	RF - 8.2.3 A (1)(A)

No.	Category	Check item	Description	Pursuant to
EI-05-50		Detecting something wrong occurs in an intrusion detection device	1. It has a function to detect something wrong occurs in an intrusion detection device.	RF - 8.2.3 A (1)(B)
EI-05-51		Alerting an administrator, when an intrusion detection device detects invasion	1. It has a function to alert an administrator when an intrusion detection device detects invasion.	RF - 8.2.3 A (1)(C)
EI-05-52		Finding the location where the invasion occurred through IDS and IPS installed	1. It has a function to find the location where the invasion occurred with IDS and IPS installed.	RF - 8.2.3 A(2)
EI-05-53		CCTV installation	1. It shall be confirmed whether CCTV has been installed.	RF - 8.2.3 B (1)(A)
EI-05-54		Real-time monitoring 24/7	1. It has a duty to use a real-time monitoring device 24/7.	RF - 8.2.3 B (1)(B)
EI-05-55		Recording all of coming and going with a CCTV system	1. It has a function to record all of coming and going out of a room with a CCTV system.	RF - 8.2.3 B (1)(C)
EI-05-56		Access control with a CCTV system	1. It has a duty to conduct access control with a CCTV system.	RF - 8.2.3 B (1)(D)
EI-05-57		Protecting a password for CCTV system administration	1. It has a duty to protect a password for CCTV system administration.	RF - 8.2.3 B (1)(E)
EI-05-58		Inquiring audit records only by right administrators	1. Possibility only for right administrators to inquire audit records.	RF - 8.2.3 B (2)(A)
EI-05-59		Searching audit records with parameters such as time, case type, etc.	1. It has a function to search audit records with parameters such as time, case type.	RF - 8.2.3 B (2)(A)

No.	Category	Check item	Description	Pursuant to
EI-05-60		Coping with the lack of storage space for audit records of an access control system	1. It has a function to figure out the lack of storage space for the audit records of an access control system.	RF - 8.2.3 B (2)(B)
EI-05-61		Access control to an entrance control system	1. It has a function to carry out access control to an entrance control system.	RF - 8.2.3 B (2)(C)
EI-05-62		Encrypting and storing a password for entrance control management system	1. It has a function to encrypt and store a password for entrance control management system.	RF - 8.2.3 B (2)(D)
EI-05-63		Backing up audit records	1. It has a function to back up audit records.	RF - 8.2.3 B (2)(E)
EI-05-64		physical security facilities controlling access to a certification system	1. It shall be confirmed whether physical security facilities have been installed to control access to a certification system.	RF - 8.2.4 A
EI-05-65		Cabinet where a locking or secure box is installed to physically control access to important data such as digital signature creation key, certificate, etc.	1. It shall be confirmed whether a cabinet with a locking or secure box is installed to physically control access to important data such as digital signature creation key, certificate has been installed.	RF - 8.2.4 B
EI-05-66		Managing a locking key in a box or cabinet with a separate locking device	1. It shall be confirmed weather a locking key in a box or cabinet with a separate locking device is managed.	RF - 8.2.4 C
EI-05-67		Installing fire-alarm devices such as smoke detection device, temperature detection device, etc.	1. It shall be confirmed whether fire-alarm devices such as smoke detection device, temperature detection device have been installed.	RF - 8.2.5 A (1)(A)
EI-05-68		Installing for coping with small-scale or big-scale fire	1. It shall be confirmed to cope with small-scale or big-scale fire.	RF - 8.2.5 A (2)(A)
EI-05-69		Copying with abnormal operations	1. It has a function to figure out abnormal operations.	RF - 8.2.5 A (2)(B)

No.	Category	Check item	Description	Pursuant to
EI-05-70		Using extinguishing material which doesn't affect other systems or devices	1. It shall be confirmed whether extinguishing material which doesn't affect other systems or devices are used.	RF - 8.2.5 A (2)(C)
EI-05-71		Installing double floors in order to protect certification system, IPS and network facilities against exposure to water	1. It shall be confirmed of double floors in order to protect certification system, IPS and network facilities against exposure to water	RF - 8.2.5 B(1)
EI-05-72		Installing power connection devices such as an outlet away from the floor	1. It shall be confirmed whether power connection devices such as an outlet is installed away from the floor.	RF - 8.2.5 B(2)
EI-05-73		A device that is able to supply power for over 30 minutes to continue certification practice when electricity fails	1. It shall be confirmed whether there is a device that is able to supply power for over 30 minutes to continue certification practice when there is electricity failure.	RF - 8.2.5 C (1)(A)
EI-05-74		In case of an independent power plant, it has a function to supply power by generating electricity for over 2 hours without an additional recharge	1. In case of an independent power plant, it has a function to supply power by generating electricity for over 2 hours without an additional recharge.	RF - 8.2.5 C (1)(B)
EI-05-75		A thermo-hygrostat to keep temperature and humidity at a specific point	1. It shall be confirmed whether a thermo-hygrostat to keep temperature and humidity at a specific point.	RF - 8.2.5 D
EI-05-76		Grounding power devices used in physical security equipment	1. It shall be confirmed whether power devices used in physical security equipment are grounded.	RF - 8.2.5 E(1)
EI-05-77		Installing induction lights and signs on emergency physical security equipment	1. It shall be confirmed whether there are induction lights and signs on emergency physical security equipment.	RF - 8.2.5 E(2)

6. User facilities

No.	Category	Check item	Description	Pursuant to
EI-06-01	Functions to manage digital signature keys	Generating a digital signature key by using a digital signature algorithm as prescribed in 5.1.1	1. It has a function to generate a secure key.	RF - 9.1.1 A
EI-06-02		Encrypting a digital certificate creation key as PKCS#5	1. It has a function to encrypt a digital certificate creation key as PKCS#5.	RF - 9.1.2 A
EI-06-03		Using an encryption algorithm as prescribed in 5.1.3 to encrypt a digital signature creation key	1. It has a function to use an encryption algorithm whose security has been proved (SEED or 3DES) to encrypt a digital signature creation key.	RF - 9.1.2 B
EI-06-04		Storing a PKCS#5-encrypted digital signature creation key as a PKCS#8 format	1. It must comply with a PKCS#8 format when storing a digital signature creation key encrypted.	RF - 9.1.2 C
EI-06-05		Complying with 6.1 of the [Annex 2] regarding storing a digital signature creation key	1. It must comply with 6.1 of the [Annex 2] regarding storing a digital signature creation key.	RF - 9.1.2 D
EI-06-06	Functions to manage certificates	Removing a digital signature key from a memory or temporary file after the digital signature creation key created has been stored into a specific storage medium	1. It has a function to automatically remove a digital signature key from memory as soon as the key has been stored into a storage medium. 2. It has a function to automatically remove an encryption key used to encrypt a digital signature key from a memory.	RF - 9.1.3 D
EI-06-07		Complying with 3.1 of the [Annex 2, certification scheme's technical standards] to generate a CSR (certificate signing request)	1. It has a function to create a CSR pursuant to the wired/wireless CSR of a digital signature certification scheme. 2. It has a function to process a server's response regarding the CSR. 3. It has a function to support DER or Base64 as a coding format to create the CSR.	RF - 9.2.1 A

No.	Category	Check item	Description	Pursuant to
EI-06-08		Complying with 3.2 of the [Annex 2, certification scheme's technical standards] on requesting for issuance, reissuance, renewal, suspension or revocation through an information network	1. It has a function to create a CSR pursuant to a wired/wireless certificate management protocol. 2. It has a function to process a server's response regarding the wired/wireless certificate management protocol. 3. It has a function to support DER or Base64 as a coding format when creating each format.	RF - 9.2.1 B
EI-06-09		Complying with 6.1 of the [Annex 2, certification scheme's technical standards] to store a subscriber's certificate	1. It has a function to comply with 6.1 of the [Annex 2, certification scheme's technical standards] to use a subscriber's certificate for cross-certification between accredited certification authorities.	RF - 9.2.2 A
EI-06-10		Certificate inquiry	1. It has a function to inquire a certificate (algorithm, key length, DN, validity, etc.) 2. It has a function to support DER or PEM as coding format when processing a certificate.	RF - 9.2.3 A
EI-06-11		Complying with 1.4 of the [Annex 2, certification scheme's technical standards] to display a certificate mark	1. It has a function to display a certificate mark.	RF - 9.2.3 B
EI-06-12		Complying with 6.1 of the [Annex 2, certification scheme's technical standards] to deliver digital signature key and certificate	1. It has a function to export/import certificate and digital signature key by using a PKCS#12.	RF - 9.2.4 A
EI-06-13		Complying with 5.2 or 6.1 of the [Annex 2, certification scheme's technical standards] in order to confirm whether the certificate of a root CA is reliable	1. It shall comply with 5.2 or 6.1 of the [Annex 2, certification scheme's technical standards] in order to confirm whether the certificate of a root CA is reliable.	RF - 9.2.5 A

No.	Category	Check item	Description	Pursuant to
EI-06-14		Setting a certificate path	1. It has a function to set the chain from the root CA certificate to a user certificate.	RF - 9.3.1 A
EI-06-15		Confirmation of certificate suspension or revocation lists	1. It has a function to verify the validity of a certificate by acquiring CRL or ARL.	RF - 9.3.1 B(1)
EI-06-16	Functions to verify digital signature and certificates	Complying with 5.3 of the [Annex 2, certification scheme's technical standards] to use an OCSP (On-line Certificate Status Protocol) service	1. It has a function to create a request message pursuant to the message format of RFC 2560. 2. It has a function to compare the request and its response by using nonce to cope with replay attacks. 3. It has a function to use HTTP as a protocol sending a request message to inquire the status of a certificate. 4. It has a function to process the Id-ad-o cps value of the extension field "Authority Info" in a certificate. 5. It has a function to verify the signature of a response message and to verify the certificate of an OCSP server that the response message is included in. 6. It has a function to verify the status of a certificate by using an OCSP.	RF - 9.3.1 B(2)

No.	Category	Check item	Description	Pursuant to
EI-06-17		Complying with 5.4 of the [Annex 2, certification scheme's technical standards] to verify the certificate path	1. It has a function to verify the digital signature signed in a certificate. 2. It has a function to compare the current system time and the valid beginning time and valid end time of a certificate. 3. It has a function to confirm the issuer of a certificate. 4. It has a function to verify the status of a certificate. 5. It has a function to confirm the usage of a certificate. 6. It has a function to confirm whether the entity is a correct certification authority and to limit the length of the certificate path. 7. It has a function to verify the certificate from a certification center with top-down certificate verification.	RF - 9.3.1 C
EI-06-18		Digital signature creation and verification	1. It has a function to create a digital signature. 2. It is a function to verify a digital signature.	RF - 9.3.2
EI-06-19		Complying with 1.5 of the [Annex 2, certification scheme's technical standards] in order to carry out identification by using a DN	1. It has a function to create a 160-bit random number. 2. It has a function to meet a FIPS PUB 140-1 standard 4.11.1 random test. 3. It has a function to share the random number with an accredited certification authority in a safe manner. 4. It shall comply with technical standards sending the random number and the format used to store the random number in an available storage medium. 5. It has a function to delete all information used to create the random number after the random number has been stored in a medium. 6. It has a function to deliver the random number when exporting or importing certificate and digital signature key.	RF - 9.4.1

No.	Category	Check item	Description	Pursuant to
			7. It has a function to update the random number when renewing the digital signature key of a subscriber. 8. It has a function to confirm identification information included in the subscriber's certificate.	
EI-06-20	Time stamping	Generating a hash value for a document that will be time-stamped	1. It generates a hash value for a document that will be time-stamped.	RF - 9.5.1 A(1)
EI-06-21		Generating a time-stamping request format pursuant to 4.2 of the [Annex 2, certification scheme's technical standards]	2. It has a function to generate a time-stamping request format pursuant to 4.2 of the [Annex 2, certification scheme's technical standards].	RF - 9.5.1 A(2)
EI-06-22		Receiving a time-stamping token for respective requests	1. It has a function to receive a time-stamping token for each request.	RF - 9.5.1 B
EI-06-23		Verifying time-stamping tokens	1. It has a function to verify time-stamping tokens.	RF - 9.5.1 C
EI-06-24		Searching by connecting the time-stamping token with the original file	1. It has a function to search by connecting the time-stamping token with the original file.	RF - 9.5.1 D(1)
EI-06-25	Configuration management of user software	Checking the version of subscriber's software provided by the accredited certification authority	1. It has a function that check subscriber's software version.	RF - 9.6.1
EI-06-26		Distributing software to subscribers when the software has been modified	1. It has a function to distribute software to subscribers in a secure manner when the software is modified.	RF - 9.6.2
EI-06-27		Coping with forgery, alteration or deletion of the subscriber software	1. It has a function to figure out alteration by hashing or digitally signing software.	RF - 9.6.3

[Annex 2] Certification scheme's technical standards

The details for each section are provided from the root ca webpage of Cameroon Root Certification Authority (CamRootCA). (http://www.rootca.cm)

1. Profiles

1.1 Digital signature certificate profile

Wired	. CCAC.TS.CERTPROF, "Digital Signature Certificate Profile"
Wireless	. CCAC.TS.WCERTPROF, "Wireless Digital Signature Certificate Profile"

1.2 Accredited digital signature certificate revocation list profile

Wired	. CCAC.TS.CRLPROF,"Digital Signature Suspension and Revocation Profile"
Wireless	. CCAC.TS.WCRLPROF, "Wireless Digital Signature Suspension and Revocation Profile"

1.3 Distinguished Name (DN) specification

Common	. CCAC.TS.DN, "Digital Signature Certification Scheme DN“

1.4 Mark specification for accredited certificates

Common	. CCAC.TS.NSACA, "Mark Specification for Accredited Certificates"

1.5 Subscriber identification based on distinguished numbers

Common	. CCAC.TS.SIVID, "Subscriber identification based on distinguished numbers“

2. Algorithms

2.1 Digital signature algorithm specification

Wired	RSA	. RSA Laboratories PKCS#1, "RSA Cryptography Specifications" . ANSI X9.31, "Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)"
	KCDSA	. TTAS.KO-12.0001/R1, "Additional Digital Signature - Second part: Certificate-based Digital Signature Algorithm"
Wireless	RSA	. RSA Laboratories PKCS#1, "RSA Cryptography Specifications" . ANSI X9.31, "Digital Signatures Using Reversible Public Key Cryptography for Financial Services Industry (DSA)"
	ECDSA	. ANSI X9.62, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA)"
Common	. KCAC.TS.DSIG, "Digital Signature Algorithm"	

2.2 Hash algorithm specification

Wired	SHA-1	. FIPS PUB 180-1, "SECURE HASH STANDARD"
	HAS-160	. TTAS.KO-12.0011/R1, "Hash Function - 2nd : Hash Algorithm Specification (AS-160)"

Wireless	SHA-1	.FIPS PUB 180-1, "SECURE HASH STANDARD"

2.3 Encryption algorithm scheme specification

Common	3-DES	.FIPS PUB 46-3, "DATA ENCRYPTION STANDARD(DES)"
	SEED	.TTAS.KO-12.0004, "128-Bit Block Encryption Algorithm Specification"

3. Management protocols

3.1 Accredited certificate request message format specification

Wired	Online	.CCAC.TS.CRMF, "Accredited Certificate Request Format Protocol Specification“
	Offline	.RSA Laboratories PKCS#10, "Certification Request Syntax Standard"
Wireless	Online	.CCAC.TS.WCRMF, "Wireless Certificate Request Format Protocol Specification“ .CCAC.TS.CRMF, "Certificate Request Format Protocol Specification“
	Offline	.RSA Laboratories PKCS#10, "Certification Request Syntax Standard"
Common	.CCAC.TS.RS, "Reference Number/Authentication Code Technical Specification for Accredited Certificate Issuance“	

3.2 Accredited certificate management protocol specification

Wired	.CCAC.TS.CMP, "Accredited Certificate Management Protocol Specification“
Wireless	.CCAC.TS.WCMP, "Wireless Certificate Management Protocol Specification“ .CCAC.TS.CMP, "Accredited Certificate Management Protocol Specification“

4. Operation protocols

4.1 LDAP specification

Common	.CCAC.TS.LDAP “LDAP Specification"

4.2 Time-Stamp protocol specification

Common	.IETF RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamping Protocol (TSP)"

4.3 Network time protocol specification

Common	.IEFT RFC 1305, "Network Time Protocol(v3) Specification, Implementation and Analysis"

5. Path validation and verification protocols

5.1 The CTL technical specification for interoperability

Wired	. CCAC.TS.CTL, “The CTL Technical Specification for Interoperability of Certification Authorities”

5.2 Root CA reliability specification

Wired	. CCAC.TS.TCI, “Root CA Certificate Reliability Specification for the Wireless Environment”

5.3 Online Certification Service Protocol

Common	. CCAC.TS.OCSP, "Online Certificate Status Protocol's Technical Specification"

5.4 Accredited certificate path validation specification

Common	. CCAC.TS.CERTVAL, "Accredited Certificate Path Validation Specification"

6. Others

6.1 User interface technical specification

Wired	. CCAC.TS.UI, "User Interface Specification for the Interoperability between Accredited Certification Authorities"

6.2 HSM storage format specification for accredited certificate

Wired	. CCAC.TS.PKCS#15, "PKCS#15 Technical Specification for Encryption Tokens“

6.3 Application interface's technical specification for HSM tokens

Wired	. CCAC.TS.PKCS#11, “PKCS#11 Specification for Hardware Security Module”

6.4 Cryptographic key protection specification

Common	. CCAC.TS.KP, “Cryptographic Key Protection Specification”

6.5 WTLS certificate technical specification

Wireless	. CCAC.TS.WTLS, "Wireless WTLS Certificate Profile“ . CCAC.TS.WTLS-DN, "Wireless WTLS Certificate DN Technical Specification“

6.6 Key distribution algorithm's technical specification

Wireless	. CCAC.TS.DSAlg, "Key Distribution Algorithm's Technical Specification“

[Annex 3] The results on actual test

1. Actual test (summarized)

Category	Audit item	Check item[1]	Detail item[2]	Result			
				Excepted	Audited	Confirmed	Needed to improve
EI-01	Facilities to manage user registration information	12	29				
EI-02	Facilities to create and manage digital signature keys	36	77				
EI-03	Facilities to create/issue/manage certificates	55	113				
EI-04	Time-stamping facilities	19	27				
EI-05	Protective facilities	77	79				
EI-06	User facilities	27	52				
Total		327	565				

1) Check items pursuant to "The Rules of Accredited Certification Authority's Facilities and Equipment"

2) Detailed check items pursuant to "The Rules of Accredited Certification Authority's Facilities and Equipment"

The List of Contributors who wrote "the Rules of Accredited Certification Authority's Facilities and Equipment"

Section	Name	Department	Company
Proposal			
Review and Writing			
Edition			