iTrust Signature Certification Authority

Certification Practice Statement

Version 1.2.2

Cybertrust Japan Co., Ltd.

April 11, 2023

Revision History

Version	Date	Reason for Revision
1.0	March 2, 2018	▪ Creation of first version Opening of iTrust Signature Certification Authority (Root Certification Authority, Intermediate Certification Authority)
1.1	January 11, 2019	▪ Changed URL of WebTrust for CA in “1.1 Overview” ▪ Changed Name of Contact Information in “1.5.2 Contact Point” ▪ Changed due to addition in case the subscriber generates the private key using HSM Added the case of HSM in “3.2.1 Method to Prove Possession of Private Key” Added the case of HSM in “6.1.2 Delivery of Subscriber’s Private Key” Added the case of HSM in “6.1.3 Delivery of Subscriber’s Private Key to Certification Authority” Added the case of HSM in “4.4.1 Certificate Acceptance Verification Procedures” Added the case of HSM in “9.6.3 Representations and Warranties of Subscribers” Fixed description of HSM in “6.1.1 Key Pair Generation” ▪ Excluded “a sole proprietor” from Subscriber ▪ Changed the definition of Serial Number of Personal Signature Certificate in “3.1.2 Need for Names to be Meaningful”
1.2	August 23, 2019	▪ Modified the description in "4.4.1 Certificate Acceptance Verification Procedures" ▪ Made other corrections of descriptions and errors
1.2.1	January 19, 2023	▪ Changed title and chapter number to conform to RFC3647 ▪ Added definition of serialNumber and of subjectAltName to Personal Signature Certificates in “3.1.2 Need for Names to be Meaningful” ▪ Modified the description in “3.1.3 Anonymity or Pseudonymity of Subscribers” ▪ Modified the description in “3.1.6 Recognition, Authentication, and Role of Trademarks” ▪ Add validation methods for CommonName (CN) and Organization Unit (OU) in “3.2.2.1 Verification of Identity” ▪ Add confirmation method in “3.2.2.2 DBA/Tradename” ▪ Modified the description in “3.2.4 Non-verified Subscriber Information” ▪ Modified evaluation items in “3.2.2.4 Data Source Accuracy” ▪ Added identity verification method of Personal Signature Certificates and verification method of organizational attributes in “3.2.3 Authentication of Individual Identity” ▪ Added verification method of application supervisor of Personal Signature Certificates in “3.2.5 Verification of Application Supervisor” ▪ Modified the description in “3.3 Identification and Authentication for Re-Key Requests” ▪ Add the procedure on acceptance of Personal Signature Certificates in “4.4.1 Conduct Constituting Certificate Acceptance” ▪ Modified the description in “4.6 Certificate Renewal” ▪ Modified and added reasons of revocation in “4.9.1.1 Reason of Revocation by Subscriber” ▪ Modified and added reasons of revocation in “4.9.1.2 Reason of Revocation by the Certification Authority” ▪ Added definition of subjectAltName and profile of organizational attributes to profile of Personal Signature Certificates in “Appendix B: Profile of Certificate” ▪ Minor modifications on other phraseologies, etc.

1.2.2	April 11, 2023	▪ Modified the cryptographic algorithm name and Object ID used for signing CRL in "Appendix B: Profile of Certificate"

Contents

1. Introduction

1.1 Overview

Cybertrust Japan Co., Ltd. (“Cybertrust”) will issue “iTrust signature certificates” in the iTrust service (unless separately provided for herein, “certificate(s)” or “subscriber certificate(s)”).

Subscriber certificates are certificates in use for signing electronic documents and are respectively issued and provided for corporations and individuals.

Cybertrust will operate the Cybertrust iTrust Root Certification Authority (“Root Certification Authority”) and the Cybertrust iTrust Signature Certification Authority (“Certification Authority”) as the subordinate Certification Authority thereof, and a subscriber certificate shall be issued by the Certification Authority.

Name of Certification Authority	Cybertrust iTrust Root Certification Authority
Serial Number of Certification Authority Certificate	09 8e a5 03 20 ee 95 3b b7 b1 a4 88 4d 8c 6f d1 63 1f 8f c2
Valid Term of Certification Authority Certificate	February 19, 2018 to February 19, 2043
Signature Algorithm	SHA2 with RSA
Key Length of Certification Authority	3072 bit
Fingerprint (SHA1)	d8 84 ef 31 b8 5c db cb 0f 95 a6 f4 cd 03 8f 88 48 13 5d 25

Name of Certification Authority	Cybertrust iTrust Signature Certification Authority
Serial Number of Certification Authority Certificate	72 4a bf c5 ea 71 1a 5b 7a 64 52 26 34 3b fd ab 3a d9 07 7f
Valid Term of Certification Authority Certificate	February 20, 2018 to February 20, 2028
Signature Algorithm	SHA2 with RSA
Key Length of Certification Authority	2048 bit
Fingerprint (SHA1)	e0 54 57 f9 f8 55 ee e0 94 55 29 e5 57 ac 89 3d d6 b6 ed
Certificates to be Issued to Subscriber	Signature Certificates
Root Certification Authority	Cybertrust iTrust Root Certification Authority

The Certification Authority and the Root Certification Authority are compliant with the following rules and laws and ordinances in order to issue certificates:

- WebTrust Principles and Criteria for Certification Authorities;
- iTrust Signature Certification Authority Certification Practice Statement;
- Adobe Approved Trust List Technical Requirements; and
- laws of Japan that are applicable to the operations to be performed by the Certification Authority established in Japan.

The Certification Authority and the Root Certification Authority are compliant with the latest version of the WebTrust Principles and Criteria for Certification Authorities (“WebTrust for CA”) published in https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria. If there is any discrepancy between this “Certification Practice Statement” (“this CPS”) and the WebTrust for CA, the WebTrust for CA shall prevail.

This CPS prescribes the requirements for the Certification Authority to issue certificates. The requirements include obligations of the Certification Authority, obligations of subscribers, and obligations of relying parties.

Upon specifying the various requirements in this CPS, the Certification Authority shall adopt the RFC3647 "Certificate Policy and Certification Practices Framework" set forth by the IETF PKIX Working Group. RFC3647 is an international guideline that sets forth the framework of CPS or "Certificate Policy" ("CP"). Matters that do not apply to the Certification Authority in the respective provisions of this CPS provided based on the framework of RFC3647 will be indicated as "Not applicable".

The Certification Authority will not individually prescribe a CP, and this CPS shall include the CP.

1.2 Document Name and Identification

The official name of this CPS shall be the "iTrust Signature Certification Authority Certification Practice Statement".

The object identifier (OID) to be assigned to this CPS and related services shall be as follows.

OID	Object
1.2.392.200081.1.20.1	Cybertrust iTrust Signature Certification Authority Certificate Policy: PolicyIdentifier

1.3 PKI Participants

The PKI Participants described in this CPS are set forth below. Each of the relevant parties must observe the obligations set forth in this CPS.

1.3.1 Certification Authority

The Certification Authority and the Root Certification Authority set forth in "1.1 Overview" of this CPS. Each Certification Authority is composed of an Issuing Authority and a Registration Authority.

The Certification Authority and the Root Certification Authority shall be governed by the Certification Authority Supervisor set forth in "5.2.1 Trusted Roles" of this CPS, and the Cybertrust Japan Policy Authority ("CTJ PA") shall approve this CPS.

1.3.2 Registration Authority

The Registration Authority of the Certification Authority is operated by Cybertrust, and accepts applications for certificates from subscribers, and screens the applications based on this CPS. Based on the validation results, the Registration Authority instructs the Issuing Authority to issue or revoke the certificates of subscribers or dismisses the applications.

1.3.3 Issuing Authority

The Issuing Authority of the Certification Authority is operated by Cybertrust, and issues or revokes certificates of subscribers based on instructions from the Registration Authority of the Certification Authority. The Issuing Authority also controls the private key of the Certification Authority based on this CPS.

1.3.4 Subscriber

A subscriber is an organization or an individual (natural person) that applies for a certificate with the Certification Authority, and uses the certificate based on this CPS and the subscriber agreement.

A person who is responsible for applying for a certificate in the organization to use the certificate is referred to as an application supervisor. A subscriber as an organization must appoint an application supervisor among persons affiliated with the subscriber's organization.

Persons affiliated with the subscriber who may apply for a certificate in the organization to use the certificate shall be limited to the application supervisor, or a procedural manager who is authorized by the application supervisor to submit an application. The procedural manager may be appointed among persons inside or outside the subscriber's organization. When the procedural manager is to be appointed from the outside, the procedural manager may be an individual or an organization. The procedural manager appointed among persons outside the subscriber's organization may be defined as the "Applicant's Agent" in the subscriber agreement and other rules.

With regard to an individual or a sole proprietor using a certificate, the application supervisor shall be the subscriber himself/herself, and the person who may apply for a certificate shall be limited to the subscriber himself/herself.

1.3.5 Relying Parties

A relying party is an organization or an individual that verifies the validity of the certificates of the Certification Authority and subscribers and relies on the certificates the Certification Authority and subscribers based on one's own judgment.

1.3.6 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

1.4.1.1 Root Certification Authority Certificate

Certificate of the Root Certification Authority indicated in Appendix B of this CPS.

1.4.1.2 Certification Authority Certificate

Certificate of the Certification Authority indicated in Appendix B of this CPS. The Certification Authority Certificate shall be issued by the Root Certification Authority.

1.4.1.3 Certificate

Uses of a certificate shall be as set forth below.

(1) Corporate Signature Certificate

- authentication of organization to use a Corporate Signature Certificate; and
- electronic signature of an electronic document.

(2) Personal Signature Certificate

- authentication of individual to use a Personal Signature Certificate; and
- electronic signature of an electronic document.

1.4.2 Prohibited Certificate Uses

The Certification Authority prohibits the use of certificates for any purpose other than as set forth in “エラー! 参照元が見つかりません。 Appropriate Certificate Uses” of this CPS.

1.5 Policy Administration

1.5.1 Organization Administering the Documents

This CPS and the subscriber agreement will be administered by the Certification Authority.

1.5.2 Contact Person

The Certification Authority will accept inquiries related to the services provided by Cybertrust and this CPS at the following contact information.

Contact Information
Cybertrust Japan Co., Ltd. iTrust Support Desk Address: 13F SE Sapporo Bldg., 1-1-2 Kita 7-jo Nishi, Kita-ku, Sapporo-shi 060-0807 Tel: 011-708-5283 Business Days: Monday to Friday (excluding National Holidays, and the designated days addressed on Cybertrust's website including Year-End and New Year) Business Hours: 9:00 to 18:00 Inquiries and complaints: As indicated below

Description	Address
▪ Inquiries regarding the application process for issuance and technical inquiries ▪ Other inquiries regarding this CPS, etc.	itrust_support@cybertrust.co.jp
▪ Inquiries regarding revocation requests and application process ▪ Inquiries regarding problems with certificates or upon discovery of fraudulent certificates ▪ Communication of other complaints	itrustca@cybertrust.co.jp

1.5.3 Person Determining CPS Suitability for the Policy

The suitability of this CPS shall be determined by CTJ PA.

1.5.4 CPS Approval Procedures

The suitability shall be approved by CTJ PA during the assessment/approval procedures prescribed in Cybertrust's internal rules.

1.6 Definitions and Acronyms

As prescribed in Appendix A of this CPS.

2. Publication and Repository Responsibilities

2.1 Repositories

Repositories of the Certification Authority will be controlled by Cybertrust.

2.2 Publication of Certification Information

The Certification Authority will publish the repositories as follows.

Publish the following information on https://www.cybertrust.ne.jp/itrust/repository/index.html:

- this CPS;
- subscriber agreement;
- other terms and conditions regarding the services of the Certification Authority ("Related Rules");
- information regarding certificates of the Root Certification Authority; and
- information regarding certificates of the Certification Authority.

Publish the following information on http://crl.itrust.ne.jp/CybertrustiTrustRootCA/cdp.crl:

- Certificate revocation list ("ARL") of subordinate Certification Authority Certificates issued by the Root Certification Authority

Publish the following information on http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl:

- Certificate revocation list ("CRL") of certificates issued by the Certification Authority

Publish the following information on http://crl.itrust.ne.jp/CybertrustiTrustRootCA/circa.crt:

- Certificates of the Root Certification Authority

Publish the following information on http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt:

- Certificates of the Certification Authority

2.3 Time and Frequency of Publication

The timing and frequency of publication regarding the information to be published by the Certification Authority shall be as follows; save for cases where repository maintenance or the like is required, but ARL and CRL shall be published 24 hours:

- publication of repositories shall be maintained 24hours a day, 7days a week;
- this CPS, the subscriber agreement, and the Related Rules shall be published each time they are amended;
- the CRL shall be renewed according to the cycle prescribed in "4.9.7 CRL Issuance Frequency" of this CPS and then published; and
- certificates of the Certification Authority and the Root Certification Authority shall be published at least during the valid term.

2.4 Access Control on Repositories

The Certification Authority shall not perform special access control on the repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Subscribers will be identified based on the X.500 Distinguished Name ("DN") in the certificate.

3.1.2 Need for Names to be Meaningful

The name included in the DN of the certificate and the name included in subjectAltName shall have the meaning of the subsequent paragraph.

(1) Corporate Signature Certificate

DN Item	Meaning
Common Name	Name of subscriber's organization; provided, however, that the addition of a registered trademark, business division, service name, etc. of the subscriber after the name of the subscriber's organization is not prohibited
Organization	Name of subscriber's organization
Organization Unit *(arbitrary item)	Registered trademark, business division, service name, etc. of subscriber's organization
Organization Identifier	Organization identifier in which the corporate registration number (13 digits) published on the National Tax Administration Agency's "Corporate Registration Number Site" is transcribed, and "JCN" is added at the beginning (not included if the organization identifier cannot be confirmed or if the individual is a sole proprietor)
Country	Country of registered address or physical business location where business is actually conducted

The name of the subscriber's organization shall be a proper legal organization name that is verified with QGIS, QIIS, or a data source of a third party organization deemed to be reliable by the Certification Authority. The organization name in the case of a sole proprietor shall be the name of the sole proprietor, business name that can be verified in the business name registry, or business name that can be verified in the Notification of Commencement of Business or copies of income tax return forms. Abbreviated company names and assumed names may not be used.

The registered trademark to be added to the Organization Unit (OU) or the Common Name (CN) shall be confirmed according to the provisions of "3.2.2.2 DBA/Tradename" of this CPS.

When including a business division, a service name, or etc. of the subscriber's organization in the Organization Unit or the Common Name (CN), the relevant values shall undergo the verification indicated in "3.2.2.1 Verification of Identity" of this CPS.

(2) Personal Signature Certificate

- Personal Signature Certificate (no organizational attributes)

DN Item	Meaning
Serial Number	Identification number obtained by combining "classification symbol of identity verification documents" and "hash value of individual identification number of identity verification documents" (however, if the use of "hash value of individual identification number of identity verification documents" is difficult, the Certification Authority will separately assign, for each certificate, a unique identification number)

Surname	Subscriber's surname
Given Name	Subscriber's given name
Common Name	Subscriber's name
Country	Country of nationality or residence as validated by government ID(s)

subjectAltName Item	Meaning
Country	Country of subscriber's address (JP fixed)
State	Subscriber's address (state)
Locality	Subscriber's address (locality, street)
Date of Birth (((Organization Unit)))	Subscriber's date of birth (western calendar)
Common Name	Subscriber's name

- Personal Signature Certificate (with organizational attributes)

▪ DN Item	Meaning
Serial Number	Identification number obtained by combining "classification symbol of identity verification documents" and "hash value of individual identification number of identity verification documents" (however, if the use of "hash value of individual identification number of identity verification documents" is difficult, the Certification Authority will separately assign, for each certificate, a unique identification number)
Surname	Subscriber's surname
Given Name	Subscriber's given name
Common Name	Subscriber's name
Country	Country of nationality or residence as validated by government ID(s)

subjectAltName Item	Meaning
Organization	Name of organization with which subscriber is affiliated
Organization Identifier	Organization identifier in which the corporate registration number (13 digits) published on the National Tax Administration Agency's "Corporate Registration Number Site" is transcribed, and "JCN" is added at the beginning (not included if the organization identifier cannot be confirmed or if the individual is a sole proprietor)
State	Organization's address (state)
Locality	Organization's address (locality, street)
Organization Unit *(arbitrary item)	Business division of organization with which subscriber is affiliated
Title *(arbitrary item)	Subscriber's job title in the organization with which it is affiliated

If subjectAltName includes a kanji that is not included in the JIS level-1 kanji set and the JIS level-2 kanji set, upon confirming with the subscriber, the kanji shall be replaced with a kanji included in the JIS level-1 kanji set and the JIS level-2 kanji set. If it is not possible to replace the kanji, or if the subscriber does not wish to replace the kanji, such kanji shall be indicated in hiragana or katakana.

The name of the subscriber's organization shall be a proper legal organization name that is verified with QGIS, QIIS, or a data source of a third party organization deemed to be reliable by the Certification Authority. Abbreviated company names and assumed names may not be used.

Furthermore, when including organizational attributes in the Personal Signature Certificate, the fact that the business division and title are correct, and the fact that the subscriber is the actual person affiliated with the organization and has been authorized by the representative of the organization to issue and sign electronic certificates storing the organization's information shall be validated and verified based on the method described in "3.2.2 Authentication of Individual Identity" of this CPS.

3.1.3 Anonymity or Pseudonymity of Subscribers

The anonymity or pseudonymity of subscribers is not allowed in the certificates issued by the Certification Authority.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting the DN form of certificates issued by the Certification Authority shall be pursuant to X.500.

3.1.5 Uniqueness of Names

The certificates issued by the Certification Authority can uniquely identify a subscriber based on the DN.

3.1.6 Recognition, Authentication, and Role of Trademarks

For a Corporate Signature Certificate, the addition of the subscriber's registered trademark after the name of the subscriber's organization (CN) is not prohibited. The registered trademark shall be confirmed pursuant to the provisions of "3.2.2.2 DBA/Tradename" of this CPS.

3.2 Initial Identity Validation

Authentication of the organization for issuing Corporate Signature Certificates is described in "3.2.2 Authentication of Organization Identity". Furthermore, authentication of individual identity for issuing Personal Signature Certificates is described in "3.2.3 Authentication of Individual Identity".

3.2.1 Method to Prove Possession of Private Key

The Certification Authority shall generate a subscriber's private key on behalf of the subscriber. As set forth in "6.1.2 Private Key Delivery to Subscriber" of this CPS, the Certification Authority shall deliver the private key to the subscriber, and it shall be deemed that the ownership of the subscriber's private key has been transferred from the Certification Authority to the subscriber upon confirmation of receipt, and the Certification Authority shall not be involved with the management of the subscriber's private key thereafter.

Additionally, when the subscriber generates a private key using the private key encryption module (hereafter, "HSM"), the certificate issue request (hereafter, "CSR"), which is a section of the application information from the subscriber, includes a digital signature corresponding to a public key and a private key corresponding to said public key. This Certification Authority, by verifying the digital signature using the public key included in the CSR, confirms that it is signed with the private key of the subscriber, and determines whether the subscriber possesses the secret key.

3.2.2 Authentication of Organization Identity

3.2.2.1 Verification of Identity

(1) Corporate Signature Certificate

Upon verifying information regarding the subscriber of a Corporate Signature Certificate, the Certification Authority shall use public documents and data, documents and data provided by a third party that is deemed reliable by the Certification Authority, or documents and data provided by the subscriber, as well as make inquiries to appropriate officers and employees of the subscriber's organization or to the organization configuring the subscriber. Moreover, the Certification Authority shall visit the subscriber's organization and conduct an on-site survey as needed.

However, when the documents and data for verifying information regarding the subscriber have been screened by the Certification Authority and a given period of time (period predetermined by the Certification Authority) has not elapsed from such validation, the Certification Authority may use such information for the verification of subscribers.

Details regarding the verification procedures to be requested to subscribers shall be posted on Cybertrust's website or notified individually to the subscribers.

The Certification Authority shall screen and verify the following matters based on the foregoing information:

- legal or physical existence of subscribers (name of organization, address of organization, corporate registration number);
- employment of the application supervisor;
- acceptance of the subscriber agreement;
- approval of the application supervisor for the procedural manager to submit an application (when the certificate request is to be submitted by the procedural manager);
- authenticity of the respective items included in the DN (excluding the OU) of the subscriber certificate prescribed in (1) "Corporate Signature Certificate" of "3.1.2 Need for Names to be Meaningful" of this CPS;
- any of the following information is not included in the organizational unit (OU) included in the certificate:
  - corporate identification number;
  - a value containing a character string that indicates the corporate status such as "*Kabushiki Kaisha*" or "Co. Ltd.";
  - address (i.e., a value indicating a location);
  - a name, company name, or trademark of a party other than the applying organization, or any other value that makes reference to a natural person or a judicial person;
  - symbols including a dot, hyphen, space, and the equivalent as well as a character string consisting solely of spaces or combination of symbols and/or spaces; or
  - a character string to indicate "not applicable," "incomplete," "blank," and the equivalent indicated by "NULL," "unknown," or "N/A";
- When adding the subscriber's registered trademark after the name of the subscriber's organization in an Organization Unit (OU) or a Common Name (CN) field, the registered trademark shall be verified pursuant to the provisions of "3.2.2.2 DBA/Tradename" of this CPS.
- When adding the business division, service name, or etc. of the subscriber's organization after the name of its organization in an Organization Unit (OU) or a Common Name (CN) field, the following matters shall be verified:
  - When a business division is to be included in the Organization Unit (OU), verify that the subscriber's organization has consented to the signature by such business division, or the delegation of authority thereof has been performed, by receiving the submission of a written consent or authority of attorney affixed with the representative's seal of the organization certified with a seal registration certificate, and such seal registration certificate.
  - When a name or etc. of the service provided by the subscriber is to be included in the Organization Unit (OU), verify that the subscriber's organization has consented to the signature by the service provider, or the delegation of authority thereof has been performed, by receiving the submission of a written consent or authority of attorney affixed with the representative's seal of the organization certified with a seal registration certificate, and such seal registration certificate.
- Additional verification in cases where the application is determined to be high-risk based on the following examination:
  - Records of applications that were dismissed or records of certificates that were revoked by the Certification Authority in the past due to suspicion of fishing and other fraudulent acts or breach of this CPS or the subscriber agreement etc.

3.2.2.2 DBA/Tradename

When the subscriber's registered trademark is to be added after its organization name listed in an Organization Unit (OU) or a Common Name (CN) field of the Corporate Signature Certificate, the Certification Authority shall verify that the subscriber has the right to use such trademark etc. by using at least one of the following methods.

- Document provided by a government agency having jurisdiction over approval, or document communicated with a government agency
- Site operated or managed by a government agency in charge of managing the registration of trade names
- Data source of a third party organization deemed reliable by the Certification Authority
- Attestation letter written by an attorney, judicial scrivener, or administrative scrivener, or report issued by a certified public accountant or tax attorney

3.2.2.3 Verification of Country

The country shall be verified according to the method described in "3.2.2.1 Verification of Identity" of this CPS.

3.2.2.4 Data Source Accuracy

The Certification Authority shall evaluate the reliability of the data source to be used in the validation. In the evaluation, the following items shall be verified such as accuracy, and tolerance against change or falsification.

- The age of the information provided
- The frequency of updates to the information source
- The data provider and purpose of the data collection
- The public accessibility of the data availability
- The relative difficulty in falsifying or altering the data

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section "3.2 Initial Identity Validation" of this CPS.

3.2.3 Authentication of Individual Identity

The Certification Authority shall verify the following matters for verifying information related to the subscriber of a Personal Signature Certificate.

- Actual existence of the subscriber
- Authenticity of the subscriber's surname, first name, and country of the subscriber's address included in the DN of the subscriber certificate and the subscriber's surname, first name, date of birth, and country, state, locality, and street of the subscriber's address included in subjectAltName prescribed in (2) Personal Signature Certificate of "3.1.2 Need for Names to be Meaningful" of this CPS
- Consent to the subscriber agreement

The Certification Authority shall verify the actual existence of the subscriber by performing identity verification using any one of Items (e), (f) or (m) (indicated below) of Article 6 (Verification Method of Identification Matters of Customers, etc.), Paragraph 1 of the Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds.

However, "the customer, etc. or its representative, etc." and "the customer, etc." shall be replaced with "subscriber", "software provided by a specified business operator" shall be replaced with "software designated by the Certification Authority", and "specified transaction, etc." shall be replaced with "certificate request of a Personal Signature Certificate".

The identity verification based on a video chat permitted under the Adobe Approved Trust List Technical Requirements shall be included in Article 6 (Verification Method of Identification Matters of Customers, etc.), Paragraph 1, Item (1)(e) of the Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds.

Furthermore, the respective items included in the DN and subjectAltName of the subscriber certificate shall be verified using an identity verification document with a photo (one among a driver's license, identity number card, basic resident register card, residence card, special permanent resident certificate, and driving record certificate) provided by the subscriber which is valid at the time that the certificate is issued.

- Article 6 (Verification Method of Identification Matters of Customers, etc.), Paragraph 1, Item (1) of the Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds
  - (e) Method of receiving from the customer, etc. or its representative, etc., by using the software provided by a specified business operator, the transmission of identity verification image information (referring to image information of the physical appearance of the customer, etc. and an identity verification document with a photo taken by the customer, etc. or its representative, etc. using the foregoing software, and in which the image information of the identity verification document with a photo enables the verification of the name, address and date of birth indicated on the identity verification document with a photo, the photo attached to the identity verification document with a photo, and the thickness or other characteristics of the identity verification document with a photo)
  - (f) Method of receiving from the customer, etc. or its representative, etc., by using the software provided by a specified business operator, the transmission of identity verification image information (referring to image information of the physical appearance of the customer, etc. taken by the customer, etc. or its representative, etc. using the foregoing software), and receiving from the customer, etc. or its representative, etc. the transmission of information recorded in a semiconductor integrated circuit incorporated into the identity verification document with a photo of the customer, etc. (limited to those in which a semiconductor integrated circuit (referring to the semiconductor integrated circuit prescribed in Article 2, Paragraph 1 of the Act Concerning the Circuit Layout of Semiconductor Integrated Circuits (Act No. 43 of 1985); hereinafter the same) with information of the name, address, date of birth and photo recorded therein is incorporated into such identity verification document with a photo)
  - (m) Method of receiving from the customer, etc. the transmission of the electronic certificate for signature issued by the Japan Agency for Local Authority Information Systems based on the provisions of Article 3, Paragraph 6 of the Act on Certification Business of Japan Agency for Local Authority Information Systems Regarding Electronic Signatures (Act No. 153 of 2002; hereinafter referred to as the "Public Individual Certification Act" in this item) and information related to the specified transaction, etc. for which the electronic signature prescribed in Article 2, Paragraph 1 of the Public Individual Certification Act, which was verified based on such electronic certificate for signature, has been provided (limited to cases where the specified business operator is the signature verifier prescribed in Article 17, Paragraph 4 of the Public Individual Certification Act)
- Additional verification in cases where the application is determined to be high-risk based on the following examination:

Records of applications that were dismissed or records of certificates that were revoked by the Certification Authority in the past due to suspicion of fishing and other fraudulent acts or breach of this CPS or the subscriber agreement etc.

As a result of the subscriber sending an image, etc. of the subscriber's identity verification document with a photo to the Certification Authority for one's identity verification, the subscriber represents that, as the application supervisor, it has accepted the subscriber agreement and approved the filing of an application.

When including organizational attributes in the Personal Signature Certificate, in addition to the authentication of the individual identity described above, the Certification Authority will verify the following.

- Legal or physical existence of the organization (name of organization, address of organization, corporate registration number);
  - To be verified using the same documents and data as the Corporate Signature Certificate.
- Business division, title, subscriber's affiliation, and signing authority
  - In the case of an organization to be registered, verify that the business division and title are correct, that the subscriber is the actual person affiliated with the organization, and that the subscriber has been authorized by the representative of the organization to issue and sign electronic certificates storing the organization's information by receiving the submission of a written consent or authority of attorney affixed with the representative's seal of the organization certified with a seal registration certificate, and such seal registration certificate. When it is possible to verify the subscriber's name and address as the representative director, in the certified copy of register of the organization, submission of a written consent or authority of attorney affixed with the representative's seal and a seal registration certificate thereof shall not be required.
  - In the case of an administrative agency or a public corporation that will not be registered, verify that the business division and title are correct, that the subscriber is the actual person affiliated with the organization, and that the subscriber has been authorized by the representative of the organization to issue and sign electronic certificates storing the organization's information by receiving the submission of a written consent or authority of attorney affixed with the representative's seal. Furthermore, submission of a seal registration certificate may be substituted with the submission of materials such as a document submitted by the organization to a government agency or an official document which enable the verification of the seal impression of the representative's seal of the organization.
  - In the case of a sole proprietor, verify that the sole proprietor himself/herself coincides with the subscriber by verifying that the validation results of the authentication of the individual identity coincide with the name and address indicated in the trade name registration, Notification of Commencement of Business or copies of income tax return forms. In the case of a sole proprietor, submission of a written consent or authority of attorney affixed with the representative's seal and a seal registration certificate thereof is not required.
- Additional verification in cases where the application is determined to be high-risk based on the following examination:

Records of applications that were dismissed or records of certificates that were revoked by the Certification Authority in the past due to suspicion of fishing and other fraudulent acts or breach of this CPS or the subscriber agreement etc.

When the Certification Authority deems necessary, the Certification Authority may request the subscriber to submit additional identity verification documents, and the verification results related to the subscriber may be reused during the period prescribed by the Certification Authority.

3.2.4 Non-verified Subscriber Information

(1) Corporate Signature Certificate

The Certification Authority does not guarantee or verify that the business division or the service name, etc. included in the Organization Unit (OU) or the Common Name (CN) of the certificate does not infringes upon the rights of a third party and does not guarantee or verify the truthfulness, and accuracy of the information described in the Organization Unit (OU) or the Common Name (CN) field.

(2) Personal Signature Certificate

The Certification Authority does not guarantee or verify that the business division included in the Organization Unit (OU) or the job title included in the Title does not guarantee or verify the truthfulness, and accuracy of the information described in the Organization Unit (OU) or the Title field.

3.2.5 Validation of Authority

(1) Corporate Signature Certificate

The Certification Authority shall verify the employment of the application supervisor and the authority to submit an application on behalf of the subscriber. The Certification Authority shall additionally verify that the application supervisor has accepted the subscriber agreement and approved the filing of an application by the procedural manager by way of callback or means equivalent to callback. The phone number to be used for the callback shall be a number provided by a third party or a number included in the documents or data which were provided by the subscriber and have been deemed to be reliable by the Certification Authority.

(2) Personal Signature Certificate

The Certification Authority shall verify that the application supervisor is the subscriber himself/herself. Furthermore, as a result of the application supervisor sending an image, etc. of the identity verification document with a photo to the Certification Authority in “3.2.3Authentication of Individual Identity”, the application supervisor represents that it has accepted the subscriber agreement and approved the certificate request.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The Certification Authority shall not accept any application for the renewal of a routine key.

3.3.2 Identification and Authentication for Re-Key after Revocation

The Certification Authority shall not accept any application for the renewal of a key after revocation.

3.4 Identity Validation and Authentication for Revocation Request

When the Certification Authority receives a revocation request from a subscriber via email, the Certification Authority shall verify the identity of the person who submitted the application, that such person is authorized to submit an application, and the reason of revocation. As the verification method, the Certification Authority shall compare the information notified to the Certification Authority upon application for issuance of a certificate and the information only known to the Certification Authority and the subscriber.

Upon receiving a revocation request for a certificate of a specific subscriber other than the subscriber of that certificate, the Certification Authority shall verify the reason for the revocation request.

In either case, when the reason for the revocation request corresponds to a revocation event related to the certificate, the Certification Authority shall notify the subscriber and revoke the certificate.

The email address to be used for the revocation request is indicated in “1.5.2 Contact Person” of this CPS and Cybertrust’s website.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

(1) Corporate Signature Certificate

Persons who may apply for a Corporate Signature Certificate shall only be the application supervisor or the procedural manager.

(2) Personal Signature Certificate

Persons who may apply for a Personal Signature Certificate shall only be limited to the Subscriber.

4.1.2 Enrollment Process and Responsibilities

(1) Corporate Signature Certificate

A subscriber shall apply for a Corporate Signature Certificate upon accepting this CPS and the subscriber agreement.

Upon filing an application, a subscriber is responsible for providing true and accurate information to the Certification Authority.

The method of applying for a certificate will be posted on Cybertrust's website or explained individually to subscribers.

(2) Personal Signature Certificate

A subscriber shall apply for a Personal Signature Certificate upon accepting this CPS and the subscriber agreement.
Upon filing an application, a subscriber is responsible for providing true and accurate information to the Certification Authority.

The method of applying for a certificate will be posted on Cybertrust's website or explained individually to subscribers.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

To be performed according to the procedures prescribed in “3.2 Initial Identity Validation” of this CPS.

4.2.2 Approval or Rejection of Certificate Applications

When all requirements prescribed in “3.2 Initial Identity Validation” of this CPS are confirmed, the Registration Authority of the Certification Authority shall approve the application, and instruct the Issuing Authority to issue a certificate. The Certification Authority will not notify the subscriber of such issuance in advance.

Meanwhile, when the requirements prescribed in “3.2 Initial Identity Validation” of this CPS are not satisfied, the Certification Authority shall dismiss the application. The Certification Authority will not return the information and data provided during the application process.

When the application is withdrawn, the Certification Authority shall also dismiss such application. Information and data related to the application will not be returned.

4.2.3 Time to Process Certificate Applications

After the Registration Authority of the Certification Authority processes the application based on the provisions of “4.2 Certificate Application Processing” of this CPS, the Issuing Authority shall promptly issue a certificate.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

After the Registration Authority of the Certification Authority processes the application based on the provisions of “4.2 Certificate Application Processing” of this CPS, the Issuing Authority shall promptly issue a certificate. In addition, the Issuing Authority shall send to the subscriber the notice set forth in “4.3.2 Notification to Subscriber by the CA of Issuance of Certificate” of this CPS.

Note that the subscriber agreement of the certificate between Cybertrust and the subscriber shall come into force from the time that the subscriber applies for the issuance of a certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Promptly after the certificate is issued, the Certification Authority shall send an email to the email address designated by the subscriber at the time of application to the effect that the certificate has been issued, and the procedures required for the subscriber to accept or use the certificate. Furthermore, procedures in cases where the reception of a private key is required shall also be included in this notification.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

(1) Corporate Signature Certificate

A subscriber receives a certificate and its private key stored in a USB token compliant with the standard of FIPS 140-2 level 2 or above in accordance with the notification sent from the Certification Authority when the Certificate is issued.

When a subscriber generates the private key with HSM, a subscriber receives the certificate, based on this CPS "**エラー! 参照元が見つかりません。** Notification to Subscriber by the CA of Issuance of Certificate", by downloading at a webpage of which URL is notified in the email from the Certification Authority or by requesting through the API for the iTrust Remote Signing Service using the Request ID notified in the email from the Certification Authority.

(2) Personal Signature Certificate

In accordance with the notification of issuance sent from the Certification Authority, the subscriber shall receive the certificate and private key stored in a USB token which satisfies level 2 or higher of FIPS140-2.

4.4.2 Publication of Certificate by the CA

The Certification Authority shall not publish a subscriber certificate.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Certification Authority shall not notify the issuance of a certificate other than as prescribed in “4.3.2 Notification to Subscriber by the CA of Issuance of Certificate” of this CPS.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

A subscriber shall use its private key and certificate only for the usage set forth in “1.4.1 Appropriate Certificate Uses” of this CPS, and use for any other usage is not allowed. Moreover, a subscriber's private key and certificate only be used by the subscriber, and the subscriber must not license the use thereof to a third party.

Other obligations of a subscriber regarding the use of its private key and certificate are set forth in “9.6.3 Subscriber Representations and Warranties” of this CPS.

4.5.2 Relying Party Public Key and Certificate Usage

A relying party shall confirm, under its own responsibility, the validity of the certificate that is used by a subscriber for the usage set forth in “1.4.1Appropriate Certificate Uses” of this CPS.

Obligations of a relying party regarding the use of a subscriber’s public key and certificate are set forth in “エラー! 参照元が見つかりません。 Relying Party Representations and Warranties” of this CPS.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

The Certification Authority shall not accept any renewal of a certificate which does not involve a rekey.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

The Certification Authority shall not accept any renewal of a certificate involving a rekey.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-keying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Not applicable.

4.7.6 Publication of the Re-keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

The Certification Authority shall not accept a request for modifying a previously issued certificate.

If there is any modification to the certificate information, a subscriber must promptly submit an application to the Certification Authority for revoking the corresponding certificate.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reason of Revocation by Subscriber

In the occurrence of any one of the following events, a subscriber must submit a request to the Certification Authority for revoking the corresponding certificate:

(i) a subscriber discovers a certificate that was issued based on an application for issuance that was not approved by the subscriber;
(ii) a subscriber learns that it's private key has been compromised or there is a possibility thereof;
(iii) a subscriber learns of the unauthorized use of its private key or certificate or the possibility thereof;
(iv) there is modification to the contents of a subscriber certificate;
(v) there is inaccurate information discovered in a subscriber certificate;
(vi) a subscriber wishes to cancel the subscriber agreement executed with the Certification Authority;

(vii) a subscriber breaches its obligation under this CPS or the subscriber agreement in using the subscriber certificate;
(viii) a subscriber learns that its certificate is not compliant with this CPS; or
(ix) a subscriber learns that, with regard to a Corporate Signature Certificate, the Organization Unit (OU) included in the certificate contains a value that cannot be included in the OU indicated in "3.2.2.1 Verification of Identity" of this CPS.

4.9.1.2 Reason of Revocation by the Certification Authority

In the occurrence of any one of the following events, the Certification Authority may revoke a subscriber certificate, without having to go through "4.9.3 Procedure for Revocation Request" of this CPS, at the time that such event is discovered; provided, however, that, with regard to (ix) below, the Certification Authority may revoke the Corporate Signature Certificate on a day that is separately notified by the Certification Authority before termination of operations:

(i) a subscriber requests the Certification Authority in writing to invalidate the subscriber certificate;
(ii) a subscriber notifies Cybertrust that the original certificate request had not been authorized and does not retroactively grant authorization;
(iii) the Certification Authority learns that the subscriber's private key has been compromised or there is a possibility thereof based on reasonable evidence;
(iv) the Certification Authority obtains evidence that the subscriber certificate was misused;
(v) the Certification Authority learns that the subject information in the subscriber certificate is contrary to facts based on reasonable evidence;
(vi) a subscriber breaches this CPS or the subscriber agreement and, even after the Certification Authority sends a notice to the subscriber demanding the correction of said breach, the subscriber fails to correct the breach after the lapse of seven (7) days after the dispatch of the foregoing notice;
(vii) the Certification Authority confirms material changes in the information included in the subscriber certificate;
(viii) the Certification Authority issued a certificate without complying with regulations to be observed in issuing the certificate or without complying with this CPS (however, in the foregoing case, the Certification Authority shall accept the official application for a certificate free of charge);
(ix) the subscriber certificate needs to be revoked based on this CPS;
(x) the Certification Authority confirms that a method developed to easily calculate the private key out of corresponding public key is demonstrated or proven (for example, the Debian weak key indicated in "http://wiki.debian.org/SSLkeys") has been demonstrated or certified;
(xi) the performance of this CPS and the obligations of the subscriber or the Certification Authority based on this CPS has been delayed or obstructed due to circumstances beyond the reasonable control of the parties (including computer failure or communication failure), and consequently information of a party that relied on the certificate is severely threatened or compromised;
(xii) the Certification Authority receives a lawful and binding order from a court or an administrative agency to the effect of revoking the subscriber certificate;
(xiii) the Certification Authority terminates its certification business;
(xiv) the technical content or format of the subscriber certificate contains a risk that is unacceptable to application software vendors, relying parties or other third parties;
(xv) a subscriber fails to pay the fee of the certificate in breach of Cybertrust's prescribed billing conditions;
(xvi) in the case of a Personal Signature Certificate, the Certification Authority learns of the subscriber's death based on reasonable evidence;
(xvii) in the case of a Corporate Signature Certificate, the Certification Authority learns that a value that cannot be included in the OU indicated in "3.2.2.1 Verification of Identity" of this CPS is contained in the Organization Unit (OU) included in the certificate;
(xviii) Cybertrust cancels the subscriber agreement with a subscriber based on the subscriber agreement; or

the Certification Authority learns that the private key of the Certification Authority and the Root Certification Authority has been compromised or there is a possibility thereof.

4.9.2 Who Can Request Revocation

Persons who may request revocation shall be the application supervisor, the procedural manager, or an agent who was notified by the Certification Authority at the time of requesting the certificate and who is duly authorized by the subscriber.

4.9.3 Procedure for Revocation Request

A subscriber shall submit a revocation request via email. The revocation request must include information that is known only to the Certification Authority and the subscriber, reason of revocation, contact information and so on in accordance with instructions of the Certification Authority. The Certification Authority shall verify the reason of revocation as prescribed in “3.4 Identity Validation and Authentication upon Revocation Request” of this CPS.

After revoking the certificate, the Certification Authority shall promptly notify the subscriber to such effect. For revocations that involve the free issuance of a certificate set forth in “9.1 Fees” of this CPS, there may be cases where the notice of revocation is given together with the notice of free issuance of a certificate.

4.9.4 Revocation Request Grace Period

In the occurrence of an event corresponding to “4.9.1.1 Reason of Revocation by Subscriber” of this CPS, a subscriber shall promptly submit a revocation request.

4.9.5 Time within Which CA Must Process the Revocation Request

The Certification Authority will accept the revocation request 24 hours a day, 7days a week.

The Registration Authority of the Certification Authority shall receive the revocation request, take the procedures based on the provisions of “4.9.3 Procedure for Revocation Request” of this CPS, and thereafter promptly instruct the Issuing Authority to revoke the target Corporate Signature Certificate. After receiving the revocation instruction, the Issuing Authority shall promptly revoke the relevant Corporate Signature Certificate.

4.9.6 Revocation Checking Requirement for Relying Parties

The relying parties shall verify the certificate revocation with the CRL issued by the Certification Authority.

4.9.7 CRL Issuance Frequency

The Certification Authority will issue the CRL in a cycle of less than 24 hours.

However, when required for taking recovery measures or business continuation measures after a disaster or other reasons, there may be cases where the CRL is issued in a cycle that exceeds the foregoing issue cycle based on the business continuity plan.

4.9.8 Maximum Latency for CRLs

The valid term of the Certification Authority's CRL is 168 hours.

The Certification Authority shall publish the certificate in the repository no later than one (1) hour after the issuance thereof.

However, when required for taking recovery measures or business continuation measures after a disaster or other reasons, there may be cases where a CRL having a valid term that is longer than the foregoing valid term is stored in a backup site in advance and subsequently published based on the business continuity plan.

4.9.9 On-line Revocation/Status Checking Availability

The Certification Authority shall provide revocation information based on CRL and shall not otherwise provide revocation information online.

4.9.10 On-line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

When the Certification Authority learns that a subscriber's private key has been compromised, or there is a possibility thereof, the Certification Authority will take revocation procedures based on “4.9.3 Procedure for Revocation Request” of this CPS.

4.9.13 Circumstances for Suspension

The Certification Authority will not accept applications for suspending the certificates.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedures for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

The Certification Authority shall not provide services that will enable the verification of the certificate status other than by way of CRL.

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

The reasons for ending the use of a subscriber certificate shall be set forth in the subscriber agreement. Moreover, if a subscriber wishes to terminate the subscriber agreement midway during the valid term of the certificate, the subscriber must submit a certificate revocation request with the Certification Authority based on “4.9.3 Procedure for Revocation Request” of this CPS.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The Certification Authority system shall be installed in a facility that is not easily affected by earthquakes, fires, floods and other disasters (“Facility”; unless separately prescribed herein, the term “Facility” as used herein shall include the main site and the backup site set forth in “5.1.8 Off- Site Backup” of this CPS). The Facility shall undergo architectural measures for preventing earthquakes, fires, floods and other disasters as well as preventing unauthorized invasion. Information regarding the location of the Certification Authority shall not be indicated outside or inside the building where the Facility is located.

5.1.2 Physical Access

The Facility and the respective rooms where certification operations are performed in the Facility shall be set with a security level according to the importance of the operation, and suitable entrance/exit control shall be performed. for authentication upon entering/existing the room, an entrance/exit card or biometric identification or other implementable technological means shall be used in accordance with the security level. for entry into particularly important rooms and one or both doors of the safe used for storing the Certification Authority's system and other important assets in the same room, measures must be taken where the doors cannot be opened unless multiple persons with entrance authority are present.

The Facility and the respective rooms where certification operations are performed in the Facility shall be monitored with a monitoring system 24 hours a day, 7 days a week.

5.1.3 Power and Air Conditioning

In the Facility, power sources with necessary and sufficient capacity for operating the Certification Authority system and related equipment shall be secured. An uninterruptable power supply and a private power generator shall be installed as measures against instantaneous interruption and blackouts. Air-conditioning equipment shall be installed in the respective rooms where certification operations are performed, and this shall be duplicated in particularly important rooms.

5.1.4 Water Exposures

A water leakage detector shall be installed in the particularly important rooms in the Facility where certification operations are performed, and waterproofing measures shall be taken.

5.1.5 Fire Prevention and Protection

The Facility is of a fire-proof construction. The particularly important rooms are located within the fire retarding division, and fire alarms and automatic gas fire extinguishers shall be installed.

5.1.6 Media Storage

Mediums containing the backup data of the Certification Authority system and documents and the like used in the validation process shall be archived in a room in which only authorized personnel can enter.

5.1.7 Waste Disposal

Documents containing Confidential Information shall be disposed after being shredded with a shredder. Electronic mediums shall be physically destroyed, initialized, demagnetized or subject to other similar measures to completely erase the recorded data before being discarded.

5.1.8 Off- Site Backup

The original or copy of the private key of the Certification Authority and important assets for system recovery shall be archived in the main site, and also in a remote backup site. The locking of the safe in the backup site shall be controlled by multiple persons, and the opening/closing of the safe shall be recorded.

5.1.9 Anti-earthquake Measures

The Facility is of an earthquake-resistant construction, and the equipment and fixtures of the Certification Authority system have undergone tip-prevention measures and anti-drop measures.

5.2 Procedural Controls

5.2.1 Trusted Roles

The Certification Authority shall set forth the personnel required for operating the Certification Authority ("Certification Authority Staff") and their roles as follows.

5.2.1.1 Certification Authority Supervisor

The Certification Authority Supervisor shall govern the Certification Authority.

5.2.1.2 Issuing Authority Manager

The Issuing Authority Manager shall control the operations of the Issuing Authority of the Certification Authority.

5.2.1.3 Issuing Authority System Administrator

The Issuing Authority System Administrator shall maintain and control the Certification Authority system under the control of the Issuing Authority Manager.

5.2.1.4 Issuing Authority Operator

The Issuing Authority Operator shall assist the operations of the Issuing Authority Manager and the Issuing Authority System Administrator; provided, however, that the Issuing Authority Operator is not authorized to operate the Certification Authority system.

5.2.1.5 Registration Authority Manager

The Registration Authority Manager shall control the operations of the Registration Authority of the Certification Authority.

5.2.1.6 Registration Authority Operator Manager

The Registration Authority Operator Manager shall control the Registration Authority Operator.

5.2.1.7 Registration Authority Operator

The Registration Authority Operator shall process the applications from the subscribers under the control of the Registration Authority Manager and request the issuance or revocation of certificates to the Issuing Authority.

5.2.2 Number of Persons Required per Task

The Certification Authority shall respectively appoint two or more Issuing Authority System Administrators and Registration Authority Operators.

5.2.3 Identification and Authentication for Each Role

The Certification Authority shall establish the entrance authority of the respective rooms where certification operations are performed and the operation authority of the Certification Authority system in accordance with the respective roles. for entry into the respective rooms and upon operation of the system, an entrance/exit card, biometric identification, digital certificate, ID and password are used independently or in combination to verify and verify the identification and entrance/operation authority.

5.2.4 Roles Requiring Separation of Duties

The Certification Authority will not allow the concurrent serving of the Issuing Authority and the Registration Authority, and the Certification Authority will not allow the Certification Authority Supervisor to concurrently serve another role.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The Certification Authority Staff shall be hired and assigned based on the recruitment standards to be separately set forth by Cybertrust.

5.3.2 Background Check Procedures

The background check of employees to be assigned as the Certification Authority Staff shall be conducted based on Cybertrust's internal rules and regulations.

5.3.3 Training Requirements

The Certification Authority shall implement training requirements and procedures to all employees who will be assigned as the Certification Authority Staff. The training requirements and procedures shall include, in addition to the education of this CPS and the Related Rules, the required training requirements and procedures in accordance with the role of the Certification Authority Staff.

The validity of the training requirements and procedures shall be evaluated by the Issuing Authority Manager or the Registration Authority Manager, and retraining shall be implemented as needed.

5.3.4 Retraining Frequency and Requirements

The Certification Authority shall implement retraining requirements and procedures to the Certification Authority Staff as needed. In the least, the Certification Authority shall implement training in the occurrence of the following events:

- when this CPS, the subscriber agreement and the Related Rules are amended, and CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager or the Registration Authority Manager deems necessary;
- when CTJ PA, the Certification Authority system is changed, and the Certification Authority Supervisor, the Issuing Authority Manager or the Registration Authority Manager deems necessary; or
- when CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager, or the Registration Authority Manager otherwise deems necessary.

5.3.5 Job Rotation Frequency and Sequence

The Certification Authority shall rotate jobs of the Certification Authority Staff as needed.

5.3.6 Sanctions for Unauthorized Actions

When a Certification Authority Staff conducts an act that is in breach of this CPS and the Related Rules, Cybertrust shall promptly investigate the cause and scope of influence and impose penalty on that Certification Authority Staff in accordance with Cybertrust's work rules.

5.3.7 Independent Contractor Requirements

When Cybertrust is to assign employees of outsourcees, contract employees of dispatched employees (collectively, the “Contract Employees”) as a Certification Authority Staff, Cybertrust shall conclude a contract that clearly sets forth the details of the outsourced work, confidentiality obligation to be imposed on the Contract Employees, and penal regulations, and demand the Contract Employees to observe this CPS and Cybertrust's internal rules and regulations. When the Contract Employees conduct an act that is in breach of this CPS and Cybertrust's internal rules and regulations, penalties shall be imposed based on the foregoing contract.

5.3.8 Documentation Supplied to Personnel

The Certification Authority shall take measures so that the respective Certification Authority Staff can only refer to documents that are required according to their respective roles.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

In order to evaluate the compliance of this CPS and the suitability of security, the Certification Authority shall collect the following records as monitoring logs. The records shall include the date and time, subject of the record, and description of event.

- records of validation performed by the Registration Authority;
- records of systems that are being maintained and controlled by the Registration Authority and the Issuing Authority;
- records regarding network security;
- records regarding the entry/exit of the Facility; and
- records regarding the maintenance and control of the Facility.

5.4.2 Frequency of Processing Log

The Certification Authority shall inspect the monitoring logs prescribed in "5.4.1 Types of Events Recorded" of this CPS once a week, once a month, and once a quarter.

5.4.3 Retention Period for Audit Log

Records of the validation performed by the Registration Authority shall be archived at least 7 years after the expiration of the valid term of the certificate that was issued based on the foregoing validation.

Other records shall be archived at least 7 years.

When the monitoring logs are no longer required, the Certification Authority shall dispose such monitoring logs based on the provisions of "5.1.7 Waste Disposal" of this CPS.

5.4.4 Protection of Audit Log

The Certification Authority shall implement access control the monitoring logs so that only authorized personnel can peruse the monitoring logs. The Certification Authority shall implement physical access control to the safe, and logical access control to folders and the like in cases of electronic mediums.

5.4.5 Audit Log Backup Procedures

The Certification Authority shall acquire the backup of logs in the systems of the Registration Authority and the Issuing Authority. for paper mediums, only the original copies thereof need to be archived.

5.4.6 Audit Collection System (internal vs. external)

Systems of the Registration Authority and the Issuing Authority shall automatically collect the monitoring logs based on the function installed in the system.

5.4.7 Notification to Event-Causing Subject

The Certification Authority shall collect and inspect the monitoring log without notifying the party that caused the event.

5.4.8 Vulnerability Assessments

The Certification Authority shall receive vulnerability assessment of an outside professional and take necessary measures for correcting the vulnerability. The Certification Authority shall similarly take necessary measures when vulnerability is discovered in the monitoring log inspection.

5.5 Records Archival

5.5.1 Types of Records Archived

The Certification Authority shall archive the following information in addition to the monitoring logs prescribed in “5.4.1 Types of Events to be Recorded” of this CPS.

- certificates of the Root Certification Authority;
- certificates of the Certification Authority;
- subscriber certificate;
- CRL;
- internal audit report;
- external audit report;
- documents and data received from the subscriber at the time of application; and
- this CPS and the Related Rules.

5.5.2 Retention Period for Archive

The Certification Authority shall archive the records prescribed in “5.5.1 Types of Records Archived” of this CPS for 7 years after the valid term of the relevant certificate.

When records are no longer required, the Certification Authority shall dispose such records based on the provisions of “5.1.7 Waste Disposal” of this CPS.

5.5.3 Protection of Archive

Records shall be protected based on the same procedures as “5.4.4 Protection of Audit Log” of this CPS.

5.5.4 Record Backup Procedures

Records shall be backed up based on the same procedures as “5.4.5 Audit Log Backup Procedures” of this CPS.

5.5.5 Requirements for Time-stamping of Records

The Certification Authority shall record the drafting date or processing date on forms and the like. If the date alone will lack authenticity as a record, the time should also be recorded. Record the issued date and time for certificates of the Certification Authority and the subscribers. The Certification Authority system shall undergo necessary measures for recording the accurate date and time of the issued certificate and monitoring logs.

5.5.6 Archive Collecting System (internal or external)

Certificates shall automatically be collected based on the function of the Certification Authority system. Other paper mediums shall be collected by the Certification Authority Staff.

5.5.7 Procedures to Obtain and Verify Archive Information

The Certification Authority shall limit persons authorized to acquire and peruse records to the Certification Authority Staff, the auditor and persons authorized by CTJ PA. Validation regarding the legibility of records shall be implemented as needed.

5.6 Key Changeover

The Certification Authority will renew the key pair of the Certification Authority so that the validity of the certificates of the Certification Authority will not expire while a subscriber certificate is valid.

The certificate including the Certification Authority's renewed public key will be posted on Cybertrust's website.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

When the private key of the Certification Authority is compromised, the Certification Authority shall execute the following, and simultaneously notify the fact of such compromise to subscribers and relying parties:

- discontinuation of certification operations using the compromised private key;
- revocation of all certificates;
- investigation of the cause of compromise;
- formulation of proposed remedial measures and evaluation/approval thereof by CTJ PA;
- execution of remedial measures;
- assessment on appropriateness of resuming business operations;
- generation of new key pairs and issuance of certificates;
- resumption of certification operations (including notification to subscribers and relying parties); and
- reissuance of certificates.

When the Certification Authority suffers from a disaster, the Certification Authority shall perform recovery operations using backup hardware, software and data based on the business continuation plan prescribed in "5.7.4 Business Continuity Capabilities after a Disaster" of this CPS, exert efforts to resume the certification operations, and publish the fact of such resumption to the subscribers and relying parties when the certification operations are resumed.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When hardware, software or data is destroyed, the Certification Authority shall continue performing the certification operations by using the backup hardware, software or data.

5.7.3 Entity Private Key Compromise Procedures

In the event the private key that is being managed under the subscriber's own responsibility is compromised, or suspected of being compromised, the subscriber must take the certificate revocation procedures based on the procedures prescribed in "4.9 Certificate Revocation and Suspension" of this CPS.

The Certification Authority will revoke a subscriber certificate based on "4.9.3 Procedure for Revocation Request" of this CPS.

5.7.4 Business Continuity Capabilities after a Disaster

The Certification Authority shall separately set forth a business continuation plan regarding the recovery measures for recovering from disasters, and business continuity. The business continuation plan will define the operating procedures of recovery and resumption of all or a part (revocation processing) of the operations of the Certification Authority by using data and the like archived in the Facility.

With regard to the recovery time from disasters, the step-by-step recovery target is set forth in the business continuation plan based on investigations of the disaster situation.

5.8 CA or RA Termination

When the Certification Authority is to terminate the operations of the Certification Authority, the Certification Authority shall notify the subscribers in advance, as well as publish information to such effect on Cybertrust's website.

The information of subscribers held by the Certification Authority shall be abolished or provided to the transferee of business operations, and this shall be announced on Cybertrust's website after the termination of operations.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pairs used by the Certification Authority and the Root Certification Authority will be respectively generated based on instructions of the Certification Authority Supervisor by multiple Issuing Authority System Administrator under the control of the Issuing Authority Manager.

Upon generating the key pairs of the Certification Authority and the Root Certification Authority, a private key cryptographic module ("HSM") that satisfies the FIPS 140-2 Level 4 standard and other methods of secret sharing shall be used.

The key pairs of the Certification Authority and the Root Certification Authority shall be generated in the presence of the auditor set forth in "8.2 Auditor Requirements" and "8.3 Relation of Auditor and Auditee" of this CPS or, when the auditor is not available, by presenting to the auditor the recording of the generation procedures so as to ensure that the generation of the key pair of the Certification Authority was performed according to predetermined procedures.

6.1.2 Private Key Delivery to Subscriber

The Certification Authority shall take measures for ensuring the confidentiality and integrity of the subscriber's private key and deliver it by using the USB token of compliant with the standards of FIPS 140-2 Level 2 or above via non-transferrable registered mail when the private key is generated by the Certification Authority. The Certification Authority does not keep the subscriber's private key afterwards.

This Certification Authority is not involved with and does not deliver the subscriber's private key when the private key is generated by a subscriber via HSM.

6.1.3 Public Key Delivery to Certificate Issuer

When a subscriber's private key is to be generated on behalf of the subscriber, a subscriber's public key will be generated by the Certification Authority.

Additionally, when the subscriber generates the private key themselves based on HSM, the subscriber, after including the public key in the certificate issue request data, delivers it from the website providing Cybertrust to the Certification Authority.

6.1.4 A Public Key Delivery to Relying Parties

The Certification Authority will not deliver the public key of the Certification Authority to relying parties. The certificates of the Certification Authority including the public key of the Certification Authority will be published on Cybertrust's website.

6.1.5 Key Sizes

The key signature algorithm and key length of the certificates of the Root Certification Authority shall be as follows.

Name of Certification Authority	Signature Algorithm	Key Length
Cybertrust iTrust Root Certification Authority	SHA2 with RSA	3072 bit

The key signature algorithm and key length of the certificates of the Certification Authority shall be as follows.

Name of Certification Authority	Signature Algorithm	Key Length
Cybertrust iTrust Signature Certification Authority	SHA2 with RSA	2048 bit

The key signature algorithm and key length of the subscriber certificate shall be as follows.

Certificate	Signature Algorithm	Key Length
Subscriber Certificate	SHA2 with RSA	2048 bit

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The key usage of certificates of the Certification Authority shall be Certificate Signing and CRL Signing. The key usage of a subscriber certificate shall be Digital Signature and Non-Repudiation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module for controlling the key pairs of the Certification Authority and the Root Certification Authority shall be the HSM that satisfies the FIPS 140-2 Level 4 standard. The HSM will be controlled by the Issuing Authority.

6.2.2 Private Key (n out of m) Multi-Person Control

The private key used by the Certification Authority and the Root Certification Authority shall at all times be controlled by multiple Issuing Authority System Administrators.

6.2.3 Private Key Escrow

The Certification Authority and the Root Certification Authority will not deposit the private key used by the Certification Authority and the Root Certification Authority or the private key of subscribers.

6.2.4 Private Key Backup

The Issuing Authority System Administrator shall back up the private key of the Certification Authority and the Root Certification Authority. The private key backed up from the HSM shall be encrypted and then divided into multiple pieces, and safely archived in a lockable safe.

6.2.5 Private Key Archival

The Certification Authority and the Root Certification Authority shall not archive the private key used by the Certification Authority and the Root Certification Authority.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The Certification Authority and the Root Certification Authority transfers a copy of the private key used by the Certification Authority and Root Certification Authority, via a safe method, to the backup site. In case recovery of the Certification Authority private key is required due to an HSM fault at the Certification Authority, the system administrator of the issuing authority recovers this using the backup stored at the main site or backup site.

6.2.7 Private Key Storage on Cryptographic Module

The private key of the Certification Authority and the Root Certification Authority is generated within the HSM of the Certification Authority and is stored after being encrypted.

6.2.8 Method of Activating Private Key

The private key used by the Certification Authority and the Root Certification Authority shall be activated by multiple Issuing Authority System Administrators based procedures to be separately prescribed based on the approval of the Issuing Authority Manager. The activation operation shall be recorded.

6.2.9 Method of Deactivating Private Key

The private key used by the Certification Authority and the Root Certification Authority shall be non-activated by multiple Issuing Authority System Administrators based procedures to be separately prescribed based on the approval of the Issuing Authority Manager. The non-activation operation shall be recorded.

6.2.10 Method of Destroying Private Key

The private key used by the Certification Authority and the Root Certification Authority shall be destroyed by multiple Issuing Authority System Administrators based procedures to be separately prescribed based on the approval of the Issuing Authority Manager and according to instructions of the Certification Authority Supervisor. Simultaneously, the private key that was backed up pursuant to “6.2.4 Private Key Backup” of this CPS shall also be destroyed based on the same procedures. The destruction operation shall be recorded.

6.2.11 Cryptographic Module Rating

The Certification Authority and the Root Certification Authority shall use the HSM that satisfies the standards set forth in “6.2.1 Cryptographic Module Standards and Controls” of this CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Storage of the public key shall be carried out by storing the certificate containing that public key.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum valid terms of certificates of the Certification Authority shall be as per the following table.

Type	Private Key	Certificate
Certificates of Root Certification Authority	Not specified	300 months or less
Certificates of Certification Authority	Not specified	120 months or less
Corporate Signature Certificate	Not specified	39 months or less
Personal Signature Certificate	Not specified	39 months or less

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used by the Certification Authority and the Root Certification Authority shall be generated and set upon giving consideration so that it cannot be easily speculated.

6.4.2 Activation Data Protection

The activation data used in the Certification Authority and the Root Certification Authority shall be stored in a lockable safe in a room that is subject to entrance/exit control based on the provisions of "5.1.2 Physical Access" of this CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Certification Authority system shall perform the following as security measures:

- authentication of authority of the operator;
- identification and authentication of the operator;
- acquisition of operation logs for important system operations;
- setup of appropriate passwords and periodical modification thereof; and
- backup and recovery.

The Root Certification Authority system shall perform the following as security measures:

- authentication of authority of the operator;
- identification and authentication of the operator;
- acquisition of operation logs for important system operations; and
- interruption of access from an external network (offline operation) and system halt other when required

6.5.2 Computer Security Rating

The Certification Authority and the Root Certification Authority shall implement, in advance, installation assessment of hardware and software to be installed by the Certification Authority. The Certification Authority and the Root Certification Authority shall also continuously collect information, perform evaluations regarding the security vulnerability in the system to be used, and take necessary measures if a material vulnerability is discovered.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The construction and modification of the Certification Authority system and the Root Certification Authority system shall be performed based on provisions to be separately set forth under the control of the development supervisor appointed internally by Cybertrust. When the development supervisor deems necessary, necessary and sufficient verification shall be carried out in a testing environment to verify that there are no security-related problems.

6.6.2 Security Management Controls

The Certification Authority system and the Root Certification Authority system shall undergo necessary settings in order to ensure sufficient security. In addition to implementing entrance/exit control and access authorization control according to the security level and antivirus measures of said system, the Certification Authority and the Root Certification Authority shall continuously collect information and perform evaluations regarding the security vulnerability, and promptly take necessary measures if a material vulnerability is discovered.

6.6.3 Life Cycle Security Controls

The Certification Authority and the Root Certification Authority shall appoint a supervisor in the respective processes of development, operation, change, and disposal of the Certification Authority system and the Root Certification Authority system, formulate and evaluate the work plan or procedures, and conduct testing as needed. The respective operations shall be recorded.

6.7 Network Security Controls

The Certification Authority's system and external systems such as the internet shall be connected via a firewall or the like and be monitored by an intrusion defense system.

The Root Certification Authority system shall not be connected to an external network and shall be operated offline.

6.8 Time Stamping

The provisions of “5.5.5 Requirements for Time-stamping of Records” of this CPS shall apply correspondingly.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

7.1.2 Certificate Extensions

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

7.1.3 Algorithm Object Identifiers

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

7.1.4 Name Forms

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

The certificate policy object identifier of a subscriber certificate shall be 1.2.392.200081.1.20.1.

7.1.7 Usage of Policy Constraint Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Not applicable.

7.2 CRL Profile

7.2.1 Version Number(s)

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

7.2.2 CRL and CRL Entry Extensions

Matters regarding the certificates of the Certification Authority and subscribers are set forth in Appendix B.

8. Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

The Certification Authority will verify the Trust Service Principles and Criteria for Certification Authorities and the Adobe Approved Trust List Technical Requirements once a year, and perform a visiting audit at the timing deemed necessary by the auditor as set forth in "8.2 Identity/Qualifications of Assessor" of this CPS.

8.2 Identity/Qualifications of Assessor

A qualified outside auditor shall verify the WebTrust for CA and the Adobe Approved Trust List Technical Requirements.

8.3 Assessor's Relationship to Assessed Entity

The auditor shall be a party that is independent from the operations of the Certification Authority and capable of maintaining neutrality.

8.4 Topics Covered by Assessment

The scope of audit shall be the scope set forth in the programs of the WebTrust for CA and the Adobe Approved Trust List Technical Requirements.

8.5 Actions Taken as a Result of Deficiency

Identified matters that are discovered in the verification will be reported to CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager and the Registration Authority Manager. When the auditor, CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager or the Registration Authority Manager determines that corrective action is required, corrective action shall be taken under the control of the Issuing Authority Manager or the Registration Authority Manager.

8.6 Communication of Results

Validation results of the WebTrust for CA and the Adobe Approved Trust List Technical Requirements will be published according to the provisions of the respective rules.

9. Other Business and Legal Matters

9.1 Fees

The fees and payment method concerning the certificates issued by the Certification Authority will be notified so that a subscriber can properly verify the same such as by posting on Cybertrust's website or submitting a quote. If there is any discrepancy between the description on Cybertrust's website and the description in the quote separately submitted by Cybertrust, the descriptions of the quote shall prevail.

Moreover, if the Certification Authority is requested by a subscriber to issue a new certificate based on the following reasons within 30 days after the issuance of a certificate, the Certification Authority shall revoke the original certificate and accept the request for issuing a new certificate free of charge:

- the delivered item was defective, such as the sent USB token being damaged; or
- the Certification Authority otherwise deems that there is due cause.

9.2 Financial Responsibility

Cybertrust shall maintain a sufficient financial foundation that is required for observing the subject matter set forth in this CPS and operating the Certification Authority. Cybertrust shall also take out appropriate insurance for covering its indemnity liability.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The Certification Authority shall handle the following information as confidential information ("Confidential Information"):

- application information from a subscriber;
- information set forth in "9.4.2 Information Treated as Private" of this CPS;
- inquiry information received from a subscriber, a relying party, or other third parties; and
- information relating to the security of the Certification Authority.

9.3.2 Information Not within the Scope of Confidential Information

Of the information held by the Certification Authority, the following information shall be excluded from the scope of Confidential Information:

- information set forth in "2.2 Publication of Certification Information" of this CPS as information to be published;
- subscriber certificate;
- information which became public knowledge due to reasons other than the negligence on the part of the Certification Authority;
- information which became public knowledge without any restriction of confidentiality from a party other than the Certification Authority; and
- information for which a subscriber agreed in advance to the effect of being disclosed or provided to a third party.

9.3.3 Responsibility to Protect Confidential Information

The Certification Authority shall take measures for preventing the divulgence of the Confidential Information. The Certification Authority shall not use the Confidential Information for any purpose other than for performing its operations; provided, however, that, when disclosure of the Confidential Information is demanded in the course of judicial, administrative or other legal proceedings; or when the Confidential Information is to be disclosed to a party such as a financial advisor or a potential acquirer/acquiree that executed a confidentiality agreement with Cybertrust in relation to an acquisition/merger and/or a party such as an attorney, certified public accountant, tax attorney or the like that legally bears the confidentiality obligation, or when Cybertrust obtains the prior approval of the subscriber disclosing the Confidential Information, Cybertrust may disclose the Confidential Information to the party requesting disclosure of such Confidential Information. In the foregoing case, the party receiving the disclosure of the requested Confidential Information must not disclose or divulge such information to any third party regardless of the method thereof.

The handling of protection of personal information shall be prescribed in “9.4 Protection of Personal Information” of this CPS.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Handling of personal information held by the Certification Authority shall be set forth in the Privacy Policy that is published on Cybertrust' website (https://www.cybertrust.co.jp/corporate/privacy-policy.html).

9.4.2 Information Treated as Private

The Certification Authority shall handle, as personal information, any information that is included in the issuance of certificates and revocation requests, inquiries or the like capable of identifying a specific individual.

9.4.3 Information Not Deemed Private

The Certification Authority shall not deem, as personal information, any information other than the information set forth in “9.4.2 Information Treated as Private” of this CPS.

9.4.4 Responsibility to Protect Private Information

The responsibility of protecting the personal information held by the Certification Authority shall be as set forth in “9.4.1 Privacy Plan” of this CPS.

9.4.5 Notice and Consent to Use Private Information

Based on a subscriber's issuance application or revocation request, it shall be deemed that the Certification Authority has obtained the consent of the subscriber with regard to the Certification Authority using the personal information of that subscriber for performing its certificate issuance/revocation operations that are scheduled in this CPS and the Certification Authority conducting an audit.

Moreover, the Certification Authority shall not use the personal information acquired from a subscriber for any purpose other than for performing the certification operations; save for the cases set forth in “9.4.6 Disclosure Pursuant to Judicial or Administrative Process” of this CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

When disclosure of personal information handled by the Certification Authority is demanded in the course of judicial, administrative or other legal proceedings, Cybertrust may disclose such personal information.

9.4.7 Other Information Disclosure Circumstances

When the Certification Authority is to outsource a part of its operations, there may be cases where the Certification Authority needs to disclose the Confidential Information to the outsourcee. In the foregoing case, the Certification Authority shall include a provision in the service contract which imposes a confidentiality obligation on the outsourcee for maintaining the confidentiality of the Confidential Information.

9.5 Intellectual Property Rights

Unless separately agreed herein, all Intellectual Property Rights pertaining to the following information shall belong to Cybertrust or Cybertrust's supplier or licensor related to the Certification Authority service:

- certificates issued by the Certification Authority and certificate revocation information;
- this CPS and related documents;
- public key and private key of the Certification Authority; and
- hardware and software leased by the Certification Authority.

9.6 Representations and Warranties

The representations and warranties of the Issuing Authority, the Registration Authority, subscribers and relying parties are prescribed below. Excluding the representations and warranties of the Issuing Authority, the Registration Authority, subscribers and relying parties that are expressly prescribed in "9.6 Representations and Warranties" of this CPS, the respective parties mutually verify that they will not make any express or implied representation or warranty.

9.6.1 CA Representations and Warranties

Cybertrust represents and warrants that it bears the following obligations upon performing operations as the Issuing Authority:

- safely control the Certification Authority private key;
- perform accurate certificate issuance and revocation based on the application from the Registration Authority;
- provide revocation information by issuing and publishing CRL;
- monitor and operate the system; and
- maintain and control the repositories.

9.6.2 RA Representations and Warranties

Cybertrust represents and warrants that it bears the following obligations upon performing operations as the Registration Authority:

- perform validation of subscribers based on this CPS;
- properly handle certificate issuance applications and revocation requests to the Issuing Authority; and
- accept inquiries ("1.5.2 Contact Person") of this CPS.

9.6.3 Subscriber Representations and Warranties

A subscriber represents and warrants that it bears the following obligations:

- provide true and accurate information upon applying for the issuance of a certificate;
- comply with the usage of the certificate ("1.4.1 Appropriate Certificate Uses" of this CPS);
- refrain from using the certificate in electronic documents that are contrary to public order and morals;

- if any doubts arise in the accuracy of the information included in the certificate, refrain from using the certificate until such doubts are resolved;
- strictly manage the private key and password to ensure the confidentiality and safety thereof;
- in the case a subscriber generates the private key, the private key is managed within HSM which satisfies the standard of FIPS 140-2 level 2 or above;
- with regard to a Corporate Signature Certificate, use the certificate only for signing an electronic document created by the organization included in the Corporate Signature Certificate, and use the certificate only for the business approved by the subscriber according to the subscriber agreement;
- with regard to a Personal Signature Certificate, use the certificate only for signing an electronic document created by the individual included in the Personal Signature Certificate, and use the certificate only for the usage of the individual subscriber according to the subscriber agreement;
- in the occurrence of an event set forth in "4.9.1.1 Reason of Revocation by Subscriber" of this CPS, promptly submit an application for the revocation of the certificate;
- upon determining that the private key has been compromised or there is a possibility thereof, promptly submit an application for the revocation of the certificate ("4.9.12 Special Requirements Related to Key Compromise" of this CPS);
- refrain from using an expired certificate or a revoked certificate; and
- observe applicable laws and regulations.

9.6.4 Relying Party Representations and Warranties

A relying party represents and warrants that it bears the following obligations:

- confirm that the certificates are being used for the usage set forth in "1.4.1 Appropriate Certificate Uses" of this CPS;
- confirm the valid term and entries of certificates issued by the Certification Authority;
- verify the digital signature and verify the issuer of the certificate;
- confirm whether the certificate has been revoked based on CRL; and
- bear legal liability for situations arising from the default of obligations prescribed in this paragraph.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

The Certification Authority shall not be liable for any default based on this CPS regarding damages excluding direct damages arising in relation to the warranties set forth in "エラー! 参照元が見つかりません。 CA Representations and Warranties" and "エラー! 参照元が見つかりません。 RA Representations and Warranties" of this CPS.

The Certification Authority shall not be liable in any way for the consequences resulting from a relying party trusting the certificates of the Certification Authority and subscribers based on one's own judgment.

9.8 Limitations of Liability

Cybertrust shall not be liable in any way in the following cases in relation to the subject matter of "エラー! 参照元が見つかりません。 CA Representations and Warranties" and "エラー! 参照元が見つかりません。 RA Representations and Warranties" of this CPS:

- any damage that arises regardless of the Certification Authority of Cybertrust observing this CPS and legal regulations;

- any damage that arises due to fraud, unauthorized use or negligence that is not attributable to Cybertrust;
- damage that arises as a result of subscribers or relying parties neglecting to perform their respective obligations prescribed in "9.6 Representations and Warranties" of this CPS;
- damage that arises as a result of the key pair of the certificate issued by the Certification Authority being divulged due to acts of a third party other than Cybertrust;
- damage that arises as a result of the certificate infringing upon the copyright, trade secret or any other intellectual property right of a subscriber, a relying party or a third party; or
- damage caused by the weakening of the cryptographic strength resulting from technological advances such as improvement in the cryptographic algorithm decoding technology, or by any other vulnerability of the cryptographic algorithm.

The total amount of damages to be borne by Cybertrust against subscribers and relying parties or other third parties with regard to any and all damages arising in relation to the application, approval, trust or any other use of the certificates of the Certification Authority shall be the amount that the subscriber has paid to Cybertrust, or an amount which does not exceed 10,000,000 yen, whichever is lower.

This upper cap shall be applied to each certificate regardless of the number of digital signatures, number of transactions, or number of damages pertaining to the respective certificates, and shall be allocated in order from the claim that is made first.

Among the damages arising from any default or breach of this CPS, the subscriber agreement or the Related Rules, the Certification Authority shall not be liable for any data loss, indirect damages including lost profits, consequential damages and punitive damages to the extent permitted under the governing law set forth in "9.14 Governing Law" of this CPS.

9.9 Indemnities

At the time that a subscriber or a relying party receives or uses a certificate issued by the Certification Authority, that subscriber or relying party shall become liable for compensating any damage suffered by Cybertrust due to claims made by a third party against Cybertrust or lawsuits or other legal measures initiated or taken by a third party against Cybertrust resulting from any of the following acts conducted by the relying party, as well as become responsible for taking measures so that Cybertrust will not suffer any more damage:

- unauthorized use, falsification, or misrepresentation during the use of a certificate;
- breach of this CPS or the subscriber agreement; or
- neglect by a subscriber to preserve the private key.

The Certification Authority is not the subscriber's or relying party's agent, trustee or any other representative.

9.10 Term and Termination

9.10.1 Term

This CPS shall come into effect when approved by CTJ PA. This CPS will not be invalidated before the time set forth in "9.10.2 Termination" of this CPS.

9.10.2 Termination

This CPS shall become invalid at the time that the Certification Authority terminates its operations, excluding the cases prescribed in "9.10.3 Effect of Termination and Survival" of this CPS.

9.10.3 Effect of Termination and Survival

The provisions of 9.3,9.4,9.5,9.6,9.7,9.8,9.9,9.10.2,9.10.3,9.13,9.14,9.15, and 9.16 of this CPS shall continue to remain in force even after the termination of this CPS.

9.11 Individual Notifies and Communications with Participants

When Cybertrust is to notify subscribers individually, such notice shall be deemed to have been made when a written notice is hand-delivered, delivered via registered mail with verification of receipt, or sent via email. Moreover, notices from subscribers to Cybertrust shall all be made according to Cybertrust's prescribed method. When the notices are made in writing, and such notices shall be deemed to have arrived when such notices are sent and received by Cybertrust.

9.12 Amendments

9.12.1 Procedures for Amendment

The Certification Authority may amend this CPS as needed based on instructions from CTJ PA. CTJ PA shall approve the amendment after obtaining the evaluation of the Certification Authority Staff or the evaluation of outside professionals such as attorneys or other experts.

9.12.2 Notification Mechanism and Period

After CTJ PA approves the amendment of this CPS, the Certification Authority shall take measures to post the CPS before amendment and the CPS after amendment for a given period on the website so that the subscribers and relying parties can verify the amended contents. The amended CPS shall come into force at the time that is separately set forth by CTJ PA unless the withdrawal of the amended CPS is publicly announced by Cybertrust. If a subscriber does not request the revocation of its digital certificate within fifteen (15) days after the effectuation thereof, it shall be deemed that the subscriber has accepted the amended CPS.

9.12.3 Circumstances under Which OID Must Be Changed

Not applicable.

9.13 Dispute Resolution Provisions

Any and all disputes arising in relation to this CPS or the certificates issued by the Certification Authorities shall be submitted to the Tokyo District Court as the competent court of agreed jurisdiction for the first instance. With regard to matters that are not set forth in this CPS or when doubts arise with regard to this CPS, the parties shall consult in good faith to resolve such matters.

9.14 Governing Law

This CPS is construed in accordance with the laws of Japan, and the laws of Japan shall apply any dispute pertaining to the certification operations based on this CPS.

9.15 Compliance with Applicable Law

Not applicable.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Unless separately specified herein, the matters agreed in this CPS supersede all other agreements unless this CPS is amended or terminated.

9.16.2 Assignment

When Cybertrust is to assign this service to a third party, this CPS and the liabilities and other obligations set forth in this CPS may also be assigned to such third party.

9.16.3 Severability

Even if any provision of this CPS is found to be invalid for one reason or another, the remaining provisions shall continue to remain in force.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

In the event the performance of a part or all of the obligations under this CPS is delayed due to calamities, court orders, labor disputes, or other reasons that are not attributable to the Certification Authorities, Cybertrust shall be exempted from the performance of its obligations under this CPS during the delay period, and shall not be liable in any way against a subscriber or a third party that trusted or used a certificate.

Appendix A: List of Definitions

Term	Definition
Archive	As used herein, the term “archive” refers to the process of storing expired certificates for a predetermined period.
Cryptographic Module	Software, hardware, or a device configured from the combination of such software and hardware that is used for ensuring security in the generation, storage and use of private keys.
Suspension	Measure for temporarily invalidating a certificate during the valid term of that certificate.
Key Pair	A public key and a private key in public key cryptography. The two keys are unique in that one key cannot be derived from another key.
Key Length	A bit number that represents the key length which is also a factor in deciding the cryptographic strength.
Activation	To cause a system or device to be a usable state. Activation requires activation data, and specifically includes a PIN and pass phrase.
Subscriber Agreement	An agreement to be accepted by a subscriber to apply for and use a certificate. This CPS constitutes a part of the subscriber agreement.
Compromise	A state where the confidentiality or completeness of information that is incidental to the private key and the private key is lost.
Public Key	One key of the key pair in public key cryptography that is notified to and used by the other party (communication partner, etc.).
Revocation	Measure for invalidating a certificate even during the valid term of that certificate.
Certificate Revocation List	Abbreviated as “CRL” in this CPS. CRL is a list of revoked certificates. The Certification Authority publishes CRL so that the subscribers and relying parties can verify the validity of certificates.
Certification Operations	Series of operations that are performed during the life cycle controls of certificates. Including, but not limited to, operations of accepting issuance/revocation requests, validation operations, issuance/revocation/discarding operations, operations of responding to inquiries, billing operations, and system maintenance and management operations of Certification Authorities.
Backup Site	A facility that is separate from the main site for storing important assets of the Certification Authorities required for certificate issuance and revocation to ensure business continuity during disasters, etc.
Private Key	One key of the key pair in public key cryptography that is kept private from others.
Main Site	A facility equipped with assets of the Certification Authorities required for certificate issuance and revocation.
Deposit	As used herein, the term “deposit” refers to the processing of registering and storing a private key or a public key with a third party.
Repository	A website or system for posting public information such as this CPS and CRL.

Root CA	A superior certification authority of the Certification Authority that issues certificates of the Certification Authority.
DBA/Tradename	Doing Business As
Distinguished Name	An identifier set forth in the X.500 recommendation formulated by ITU-T. Configured from attribute information such as a common name, organization name, organizational unit name, and country name.
FIPS 140-2 Level 4	FIPS (Federal Information Processing Standards Publication 140) is a U.S. federal standard that prescribes the specifications of security requirements in a cryptographic module, and the latest version of this standard is 2. With this standard, the security requirements are classified as the levels of 1 (lowest) to 4 (highest).
IETF PKIX Working Group	Internet Engineering Task Force (IETF) is an organization that standardizes technologies used for the internet, and the PKIX Working Group of IETF set forth RFC3647.
ITU-T	Telecommunications Standardization Sector of the International Telecommunication Union.
RSA	Public key cryptography developed by Rivest, Shamir, and Adelman.
SHA1/SHA2	A hash function used in digital signatures, etc. A hash function is used for reducing data into a given length based on mathematical operations, and makes it infeasible to calculate the same output value from two different input values. It is also infeasible to inverse the input value from the output value.
Trust Service Principles and Criteria for Certification Authorities	Principles related to the operation of Certification Authorities that were formulated by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants. Formerly called WebTrust Program for Certification Authorities.
X.500	International standard of distribution directory services to be provided on a network standardized by ITU-T.
X.509	International standard of digital certificates standardized by ITU-T.
PDF	An electronic document used for electronically distributing, exchanging and accumulating information. PDF is an acronym of Portable Document Format. Documents created using document creation software are converted into PDF format and used. A PDF reader is used to read PDF documents.
Adobe Approved Trust List Technical Requirements	Technical requirements that need to be satisfied for registration in the Adobe Approved Trust List (AATL).
iTrust Remote Signing Service	A cloud service provided by Cybertrust which supports a long-term signing and ensures the authenticity of the electronized paper documents and/or the electronic documents required for the electronic contract.

Appendix B: Profile of Certificate

■Cybertrust iTrust Root Certification Authority (Signature Algorithm: SHA-2)

Certification Authority Certificate (Valid Term: February 19, 2018 to February 19, 2043)

(Standard Area)

Version		**Value**
Version	Version of certificate format Type: INTEGER Value: 2	 2 (Ver.3)
Serialnumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique integer	 *Serial number (HEX) 09 8e a5 03 20 ee 95 3b b7 b1 a4 88 4d 8c 6f d1 63 1f 8f c2
Signature		**Value**
AlgorithmIdentifier Algorithm parameters	Identifier of cryptographic algorithm used for signing certificate (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1 2 840 113549 1 1 11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value OrganizationIdentifer type value OrganizationName Type value CommonName Type value	Country name of certificate issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization identifier of certificate issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization name of certificate issuer Object ID of organization name Type: OID Value: 2.5.4.10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name of certificate issuer Object ID of common name Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString Value: Cybertrust iTrust Root Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Root Certification Authority
Validity		**Value**
Validity notBefore notAfter 	Validity period of certificate Commencement date Type: UTCTime Value: yymmddhhmmssZ Termination date Type: UTCTime Value: yymmddhhmmssZ	 *Commencement date of valid term 180219060842Z (February 19, 2018 15: 08: 42 JST) *Termination date of valid term 430219060842Z (February 19, 2043 15:08:42 JST)
Subject		**Value**

CountryName type	Country name of certificate subject Object ID of country name Type: OID Value: 2 5 4 6	 2.5.4.6
value	Value of country name Type: PrintableString Value: JP	 JP
OrganizationIdentifer type	Organization identifier of certificate subject Object ID of organization identifier Type: OID Value: 2.5.4.97	 2.5.4.97
value	Value of organization identifier Type: PrintableString Value: JCN3010401064771	 JCN3010401064771
OrganizationName type	Organization name of certificate subject Object ID of organization name Type: OID Value: 2 5 4 10	 2.5.4.10
value	Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd.	 Cybertrust Japan Co., Ltd.
CommonName type	Common name of certificate subject Object ID of common name Type: OID Value: 2 5 4 3	 2.5.4.3
value	Value of common name Type: PrintableString Value: Cybertrust iTrust Root Certification Authority	 Cybertrust iTrust Root Certification Authority
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo AlgorithmIdentifier algorithm	Public key information of certificate subject Identifier of cryptographic algorithm (public key cryptography and hash function) Object ID of cryptographic algorithm (RSA PUBLIC Key) Type: OID Value: 1 2 840 113549 1 1 1	 1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm Type: NULL Value:	 NULL
subjectPublicKey	Public key value Type: BIT STRING Value: Public key value	 Public key of 3072 bit length

(Expansion Area)

subjectKeyIdentifier (extnId: == 2 5 29 14, critical: == FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Information related to public key of certificate subject Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of subject	 f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
certificatePolicies (extnId: == 2 5 29 32, critical: == FALSE)		**Value**
PolicyInformation policyIdentifier	Policy-related information Type: OID Value: 1.2.392.200081.1.20.1	 1.2.392.200081.1.20.1
policyQualifiers policyQualifierID	Policy-related information Type of policyQualifiers Type: OID Value: Object ID of CPSuri (id-qt-cps)	 1.3.6.1.5.5.7.2.1
Qualifier	URI where CPS is published Type: OctetString Value: https://www.cybertrust.ne.jp/itrust/repository/index.html	 https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Information related to public key of certificate issuer Identifier of public key Type: OctetString	

	Value: Hash value of subjectPublicKey of issuer	f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
keyUsage (extnId: == 2 5 29 15, critical: == TRUE)		**Value**
KeyUsage	Key usage Type: BitString Value: 00000110 (keyCertSign, cRLSign)	 00000110 (0x0006)
basicConstraints (extnId: == 2 5 29 19, critical: == TRUE)		**Value**
BasicConstraints cA PathLenConstraint	Basic constraints Flag showing whether certificate is a CA Type: Boolean Value: True (certificate is a CA) Path length constraints Type: INTEGER Value: 2	 TRUE 2

■ARL

(Standard Area)

Version		**Value**
Version	Version of certificate format Type: INTEGER Value: 1	 1 (Ver.2)
Signature		**Value**
AlgorithmIdentifier algorithm parameters	Identifier of cryptographic algorithm used for signing CRL (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1.2.840.113549.1.1.11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value OrganizationIdentifer type value OrganizationIdentifer type value OrganizationName type Value CommonName type value 	Country name of CRL issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization identifier of CRL issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization identifier of CRL issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization name of CRL issuer Object ID of organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name of CRL issuer Object ID of common name Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString Cybertrust iTrust Root Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Root Certification Authority
ThisUpdate		**Value**
ThisUpdate	Issue date of CRL Type: UTCTime Value: yymmddhhmmssZ	 180219062956Z
NextUpdate		**Value**
NextUpdate	Next scheduled update of CRL Type: UTCTime Value: yymmddhhmmssZ	 (ThisUpdate + 9131 days later) 430219062956Z

(Expansion Area)

authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier	Information related to public key of CRL issuer	

keyIdentifier	Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of issuer	 f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
cRLNumber (extnId: == 2 5 29 20, critical: == FALSE)		**Value**
cRLNumber	Sequence number of revocation list Type: INTEGER Value: Unique integer	 *CRL number

(Entry Area)

RevokedCertificates		**Value**
CertificateSerialNumber	Certificate serial number Type: INTEGER Value: Unique integer	 *Serial number of revoked certificate
revocationDate	Revocation processing date Type: UTCTime Value: yymmddhhmmssZ	 *Revocation processing date

(Entry Expansion Area)

invalidityDate (extnId: == 2 5 29 24, critical: == FALSE)		**Value**
invalidityDate	Invalidity date Type: GeneralizedTime Value: yyyymmddhhmmssZ	 *Revocation processing date of certificate
cRLReason (extnId: == 2 5 29 21, critical: == FALSE)		**Value**
cRLReason	Revocation reason code Type: Enumerated Value: Revocation reason code	 *Value of revocation reason code

■Cybertrust iTrust Signature Certification Authority (Signature Algorithm: SHA-2)

Certification Authority Certificate (Valid Term: February 20, 2018 to February 20, 2028)

(Standard Area)

Version		**Value**
Version	Version of certificate format Type: INTEGER Value: 2	 2 (Ver.3)
Serialnumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique integer	 *Serial number (HEX) 72 4a bf c5 ea 71 1a 5b 7a 64 52 26 34 3b fd ab 3a d9 07 7f
Signature		**Value**
AlgorithmIdentifier Algorithm parameters	Identifier of cryptographic algorithm used for signing certificate (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1 2 840 113549 1 1 11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value OrganizationIdentifer type value OrganizationName type value CommonName Type value	Country name of certificate issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization identifier of certificate issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization name of certificate issuer Object ID of organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name of certificate issuer Object ID of common name Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString Value: Cybertrust iTrust Root Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Root Certification Authority
Validity		**Value**
Validity notBefore notAfter 	Validity period of certificate Commencement date Type: UTCTime Value: yymmddhhmmssZ Termination date Type: UTCTime Value: yymmddhhmmssZ	 *Commencement date of valid term 180220061215Z (February 20, 2018 15: 12: 15 JST) *Termination date of valid term 280220061215Z (February 20, 2028 15: 12: 15 JST)
Subject		**Value**
CountryName type value	Country name of certificate subject Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString	 2.5.4.6

	Value: JP	JP
OrganizationIdentifer	Organization identifier of certificate subject	
type	Object ID of organization identifier	
	Type: OID	
	Value: 2.5.4.97	2.5.4.97
value	Value of organization identifier	
	Type: PrintableString	
	Value: JCN3010401064771	JCN3010401064771
OrganizationName	Organization name of certificate subject	
type	Object ID of organization name	
	Type: OID	
	Value: 2 5 4 10	2.5.4.10
value	Value of organization name	
	Type: PrintableString	
	Value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	Common name of certificate subject	
type	Object ID of common name	
	Type: OID	
	Value: 2 5 4 3	2.5.4.3
value	Value of common name	
	Type: PrintableString	
	Value: Cybertrust iTrust Signature Certification Authority	Cybertrust iTrust Signature Certification Authority
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo	Public key information of certificate subject	
AlgorithmIdentifier	Identifier of cryptographic algorithm (public key cryptography and hash function)	
algorithm	Object ID of cryptographic algorithm (RSA PUBLIC Key)	
	Type: OID	
	Value: 1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm	
	Type: NULL	NULL
	Value:	
subjectPublicKey	Public key value	
	Type: BIT STRING	
	Value: Public key value	Public key of 2048 bit length

(Expansion Area)

cRLDistributionPoints (extnId: == 2 5 29 31, critical: == FALSE)		**Value**
cRLDistributionPoints	CRL distribution points	
DistributionPoint	CRL distribution points	
uniformResourceIdentifier	URI	
	Type: OctetString	
	Value: http://crl.itrust.ne.jp/CybertrustiTrustRootCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustRootCA/cdp.crl
subjectKeyIdentifier (extnId: == 2 5 29 14, critical: == FALSE)		**Value**
SubjectKeyIdentifier	Information related to public key of certificate subject	
keyIdentifier	Identifier of public key	
	Type: OctetString	
	Value: Hash value of subjectPublicKey of subject	e9 53 9f 51 b0 1e 13 38 ac 7b 6c 28 05 e0 47 52 49 ef ba ce
certificatePolicies (extnId: == 2 5 29 32, critical: == FALSE)		**Value**
PolicyInformation	Policy-related information	
policyIdentifier	Type: OID	
	Value: 1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
policyQualifiers	Policy-related information	
policyQualifierID	Type of policyQualifiers	
	Type: OID	
	Value: Object ID of CPSuri (id-qt-cps)	1.3.6.1.5.5.7.2.1
Qualifier	URI where CPS is published	
	Type: OctetString	
	Value: https://www.cybertrust.ne.jp/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier	Information related to public key of certificate issuer	
keyIdentifier	Identifier of public key	

	Type: OctetString Value: Hash value of subjectPublicKey of issuer	f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
keyUsage (extnId: == 2 5 29 15, critical: == TRUE)		**Value**
KeyUsage	Key usage Type: BitString Value: 00000110 (keyCertSign,cRLSign)	00000110 (0x0006)
basicConstraints (extnId: == 2 5 29 19, critical: == TRUE)		**Value**
BasicConstraints cA PathLenConstraint	Basic constraints Flag showing whether certificate is a CA Type: Boolean Value: True (certificate is a CA) Path length constraints Type: INTEGER Value: 1	 TRUE 1

■Corporate Signature Certificate

(Standard Area)

Version		**Value**
Version	Version of certificate format Type: INTEGER Value: 2	 2 (Ver.3)
Serialnumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique integer	 *Serial number (Unique integer)
Signature		**Value**
AlgorithmIdentifier algorithm Parameters	Identifier of cryptographic algorithm used for signing certificate (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1 2 840 113549 1 1 11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value OrganizationIdentifer type value OrganizationName type value CommonName Type Value	Country name of certificate issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization identifier of certificate issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization name of certificate issuer Object ID of organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name of certificate issuer Object ID of common name Type: OID Value: 2.5.4.3 Value of common name Type: PrintableString Value: Cybertrust iTrust Signature Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Signature Certification Authority
Validity		**Value**
Validity notBefore notAfter 	Validity period of certificate Commencement date Type: UTCTime Value: yymmddhhmmssZ Termination date Type: UTCTime Value: yymmddhhmmssZ	 *Commencement date of valid term *Termination date of valid term
Subject		**Value**
CountryName Type value OrganizationIdentifer type value	Country name of certificate subject Object ID of country name Type: OID Value: 2.5.4.6 Value of country name Type: PrintableString Value: <<Country name of subject>> Organization identifier of certificate subject Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier	 2.5.4.6 *Country name of subject 2.5.4.97

	Type: PrintableString Value:	*Organization identifier of subject
OrganizationName type	Organization name of certificate subject Object ID of organization name Type: OID Value: 2.5.4.10	2.5.4.10
value	Value of organization name Type: PrintableString / UTF8String Value: <<Company name of subject>>	*Company name of subject
OrganizationUnitName type	Organization Unit name of certificate subject Object ID of Organization Unit Type: OID Value: 2.5.4.11	*Only when required 2.5.4.11
value	Value of Organization Unit Type: PrintableString / UTF8String Value: <<Registered trademark, business division, service name, etc. of subscriber's organization>>	*Registered trademark, business division, service name, etc. of subscriber's organization
CommonName type	Common name of certificate subject Object ID of common name Type: OID Value: 2.5.4.3	2.5.4.3
value	Value of common name Type: PrintableString / UTF8String Value: <<In addition to common name of subject, registered trademark, business division, service name, etc. of subscriber's organization may be included.>>	*In addition to common name of subject, registered trademark, business division, service name, etc. of subscriber's organization may be included.
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo AlgorithmIdentifier	Public key information of certificate subject Identifier of cryptographic algorithm (public key cryptography and hash function)	
algorithm	Object ID of cryptographic algorithm (RSA PUBLIC Key) Type: OID Value: 1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm Type: NULL Value:	NULL
subjectPublicKey	Public key value Type: BIT STRING Value: Public key value	*2048bit

(Expansion Area)

basicConstraints (extnId: == 2 5 29 19, critical: == TRUE)		**Value**
BasicConstraints cA	Basic constraints Flag showing whether certificate is a CA Type: Boolean Value: FALSE (certificate is not a CA)	FALSE
certificatePolicies (extnId: == 2 5 29 32, critical: == FALSE)		**Value**
PolicyInformation policyIdentifier	Policy-related information Type: OID Value: 1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
policyQualifiers policyQualifierID	Policy-related information Type of policyQualifiers Type: OID Value: Object ID of userNotice (id-qt-unotice)	1.3.6.1.5.5.7.2.2
Qualifier	Text-based statement Type: OctetString Value: https://www.cybertrust.ne.jp/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityInfoAccess (extnId: == 1 3 6 1 5 5 7 1 1, critical: == FALSE)		**Value**
Authority Information Access Caissuers	Certification Authority information access Certification Authority access method Type: OID Value: 1.3.6.1.5.5.7.48.2 Type: OctetString Value: http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt	1.3.6.1.5.5.7.48.2 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt

keyUsage (extnId: == 2 5 29 15, critical: == TRUE)		**Value**
KeyUsage	Key usage Type: BitString Value: 11000000 (digitalSignature, nonRepudiation)	11000000 (0x00C0)
extendedKeyUsage (extnId: == 2.5.29.37, critical: == FALSE)		**Value**
extendedKeyUsage	Extended key usage Type: OID Value: 1.3.6.1.5.5.7.3.4 Type: OID Value: 1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4 (emailProtection) 1.3.6.1.5.5.7.3.3 (codeSigning)
authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Information related to public key of certificate issuer Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of issuer	
cRLDistributionPoints (extnId: == 2 5 29 31, critical: == FALSE)		**Value**
cRLDistributionPoints DistributionPoint uniformResourceIdentifie	CRL distribution points CRL distribution points URI Type: OctetString Value: http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl
subjectKeyIdentifier (extnId: == 2 5 29 14, critical: == FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Information related to public key of certificate subject Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of subject	*Hash value of subjectPublicKey of subject

■Personal Signature Certificate (no organizational attributes)

(Standard Area)

Version		**Value**
Version	Version of certificate format Type: INTEGER Value: 2	 2 (Ver.3)
Serialnumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique integer	 *Serial number (Unique integer)
Signature		**Value**
AlgorithmIdentifier algorithm Parameters	Identifier of cryptographic algorithm used for signing certificate (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1 2 840 113549 1 1 11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value OrganizationIdentifer type value OrganizationName type value CommonName Type Value	Country name of certificate issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization identifier of certificate issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization name of certificate issuer Object ID of organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name of certificate issuer Object ID of common name Type: OID Value: 2.5.4.3 Value of common name Type: PrintableString Value: Cybertrust iTrust Signature Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Signature Certification Authority
Validity		**Value**
Validity notBefore notAfter 	Validity period of certificate Commencement date Type: UTCTime Value: yymmddhhmmssZ Termination date Type: UTCTime Value: yymmddhhmmssZ	 *Commencement date of valid term *Termination date of valid term
Subject		**Value**
CountryName Type value CommonName type value	Country name of certificate subject Object ID of country name Type: OID Value: 2.5.4.6 Value of country name Type: PrintableString Value: <<Country name of subject>> Common name of certificate subject Object ID of common name Type: OID Value: 2 5 4 3 Value of common name	 2.5.4.6 *Country name of subject 2 5 4 3

	Type: PrintableString / UTF8String Value: <<Name of subject>>	*Name of subject
GivenName type	Given name of certificate subject Object ID of given name Type: OID Value: 2.5.4.42	2.5.4.42
value	Value of given name Type: PrintableString / UTF8String Value: <<Given name of subject>>	*Given name of subject
Surname type	Surname of certificate subject Object ID of surname Type: OID Value: 2.5.4.4	2.5.4.4
value	Value of surname Type: PrintableString / UTF8String Value: <<Surname of subject>>	*Surname of subject
SerialNumber type	Serial number of certificate subject Object ID of serial number Type: OID Value: 2.5.4.5	2.5.4.5
value	Value of serial number Type: PrintableString Value: <<Serial number of subject>>	*Serial number of subject
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo AlgorithmIdentifier algorithm	Public key information of certificate subject Identifier of cryptographic algorithm (public key cryptography and hash function) Object ID of cryptographic algorithm (RSA PUBLIC Key) Type: OID Value: 1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm Type: NULL Value:	NULL
subjectPublicKey	Public key value Type: BIT STRING Value: Public key value	*2048bit

(Expansion Area)

basicConstraints (extnId: == 2 5 29 19, critical: == TRUE)		**Value**
BasicConstraints cA	Basic constraints Flag showing whether certificate is a CA Type: Boolean Value: False (certificate is not a CA)	FALSE
certificatePolicies (extnId: == 2 5 29 32, critical: == FALSE)		**Value**
PolicyInformation policyIdentifier	Policy-related information Type: OID Value: 1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
policyQualifiers policyQualifierID	Policy-related information Type of policyQualifiers Type: OID Value: Object ID of CPSuri (id-qt-cps)	1.3.6.1.5.5.7.2.1
Qualifier	URI where CPS is published Type: URL Value: https://www.cybertrust.ne.jp/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityInfoAccess (extnId: == 1 3 6 1 5 5 7 1 1, critical: == FALSE)		**Value**
Authority Information Access Caissuers	Certification Authority information access Certification Authority access method Type: OID Value: 1.3.6.1.5.5.7.48.2 Type: OctetString Value: http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt	1.3.6.1.5.5.7.48.2 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt
keyUsage (extnId: == 2 5 29 15, critical: == FALSE)		**Value**
KeyUsage	Key usage Type: BitString Value: 11000000 (digitalSignature, nonRepudiation)	11000000 (0x00C0)

extendedKeyUsage (extnId: == 2.5.29.37, critical: == FALSE)		Value
extendedKeyUsage	Extended key usage Type: OID Value: 1.3.6.1.5.5.7.3.4 Type: OID Value: 1.3.6.1.5.5.7.3.3	 1.3.6.1.5.5.7.3.4 (emailProtection) 1.3.6.1.5.5.7.3.3 (codeSigning)
authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Information related to public key of certificate issuer Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of issuer	
subjectAltName (entnID: == 2 5 29 17, critical: == FALSE)		**Value**
subjectAltName	Alternative name of certificate subject	
directoryName	Directory name	
	Type: UTF8String (however, only c is PrintableString)	c = JP
	Value: "c = JP, s =, certificate subject's address (state), l = certificate subject's address (locality), ou = certificate subject's date of birth (western calendar), cn = certificate subject's name"	s = "subject's address (state)" l = "subject's address (locality, street)" ou = "subject's date of birth (western calendar)" cn = "subject's name"
cRLDistributionPoints (extnId: == 2 5 29 31, critical: == FALSE)		**Value**
cRLDistributionPoints DistributionPoint uniformResourceIdentifie	CRL distribution points CRL distribution points URI Type: OctetString Value: http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl	 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl
subjectKeyIdentifier (extnId: == 2 5 29 14, critical: == FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Information related to public key of certificate subject Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of subject	 *Hash value of subjectPublicKey of subject

■Personal Signature Certificate (with organizational attributes)

(Standard Area)

Version		Value
Version	Version of certificate format Type: INTEGER Value: 2	 2 (Ver.3)
Serialnumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique integer	 *Serial number (Unique integer)
Signature		**Value**
AlgorithmIdentifier algorithm Parameters	Identifier of cryptographic algorithm used for signing certificate (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1 2 840 113549 1 1 11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value	Country name of certificate issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP	 2.5.4.6 JP

OrganizationIdentifer	Organization identifier of certificate issuer	
type	Object ID of organization identifier Type: OID Value: 2.5.4.97	2.5.4.97
value	Value of organization identifier Type: PrintableString Value: JCN3010401064771	JCN3010401064771
OrganizationName	Organization name of certificate issuer	
type	Object ID of organization name Type: OID Value: 2 5 4 10	2.5.4.10
value	Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	Common name of certificate issuer	
Type	Object ID of common name Type: OID Value: 2.5.4.3	2.5.4.3
Value	Value of common name Type: PrintableString Value: Cybertrust iTrust Signature Certification Authority	Cybertrust iTrust Signature Certification Authority
Validity		**Value**
Validity	Validity period of certificate	
notBefore	Commencement date Type: UTCTime Value: yymmddhhmmssZ	*Commencement date of valid term
notAfter	Termination date Type: UTCTime Value: yymmddhhmmssZ	*Termination date of valid term
Subject		**Value**
CountryName	Country name of certificate subject	
Type	Object ID of country name Type: OID Value: 2.5.4.6	2.5.4.6
value	Value of country name Type: PrintableString Value: <<Country name of subject>>	*Country name of subject
CommonName	Common name of certificate subject	
type	Object ID of common name Type: OID Value: 2 5 4 3	2 5 4 3
value	Value of common name Type: PrintableString / UTF8String Value: <<Name of subject>>	*Name of subject
GivenName	Given name of certificate subject	
type	Object ID of given name Type: OID Value: 2.5.4.42	2.5.4.42
value	Value of given name Type: PrintableString / UTF8String Value: <<Given name of subject>>	*Given name of subject
Surname	Surname of certificate subject	
type	Object ID of surname Type: OID Value: 2.5.4.4	2.5.4.4
value	Value of surname Type: PrintableString / UTF8String Value: <<Surname of subject>>	*Surname of subject
SerialNumber	Serial number of certificate subject	
type	Object ID of serial number Type: OID Value: 2.5.4.5	2.5.4.5
value	Value of serial number Type: PrintableString Value: <<Serial number of subject>>	*Serial number of subject
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo	Public key information of certificate subject	
AlgorithmIdentifier	Identifier of cryptographic algorithm (public key cryptography and hash function)	
algorithm	Object ID of cryptographic algorithm (RSA PUBLIC Key) Type: OID Value: 1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm	

	Type: NULL Value:	NULL
subjectPublicKey	Public key value Type: BIT STRING Value: Public key value	*2048bit

(Expansion Area)

basicConstraints (extnId: == 2 5 29 19, critical: == TRUE)		**Value**
BasicConstraints cA	Basic constraints Flag showing whether certificate is a CA Type: Boolean Value: False (certificate is not a CA)	 FALSE
certificatePolicies (extnId: == 2 5 29 32, critical: == FALSE)		**Value**
PolicyInformation policyIdentifier policyQualifiers policyQualifierID Qualifier	Policy-related information Type: OID Value: 1.2.392.200081.1.20.1 Policy-related information Type of policyQualifiers Type: OID Value: Object ID of CPSuri (id-qt-cps) URI where CPS is published Type: URL Value: https://www.cybertrust.ne.jp/itrust/repository/index.html	 1.2.392.200081.1.20.1 1.3.6.1.5.5.7.2.1 https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityInfoAccess (extnId: == 1 3 6 1 5 5 7 1 1, critical: == FALSE)		**Value**
Authority Information Access Caissuers	Certification Authority information access Certification Authority access method Type: OID Value: 1.3.6.1.5.5.7.48.2 Type: OctetString Value: http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt	 1.3.6.1.5.5.7.48.2 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt
keyUsage (extnId: == 2 5 29 15, critical: == FALSE)		**Value**
KeyUsage	Key usage Type: BitString Value: 11000000 (digitalSignature, nonRepudiation)	 11000000 (0x00C0)
extendedKeyUsage (extnId: == 2.5.29.37, critical: == FALSE)		**Value**
extendedKeyUsage	Extended key usage Type: OID Value: 1.3.6.1.5.5.7.3.4 Type: OID Value: 1.3.6.1.5.5.7.3.3	 1.3.6.1.5.5.7.3.4 (emailProtection) 1.3.6.1.5.5.7.3.3 (codeSigning)
authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Information related to public key of certificate issuer Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of issuer	
subjectAltName (entnID: == 2 5 29 17, critical: == FALSE)		**Value**
subjectAltName	Alternative name of certificate subject	
directoryName	Directory name	
	Type: UTF8String (however, only c is PrintableString)	c = JP
	Value: “o = name of organization with which subscriber is affiliated, OID.2.5.4.97 = organization identifier of organization with which subscriber is affiliated, s = address (state) of organization with which subscriber is affiliated, l = address (locality, street) of organization with which subscriber is affiliated, ou = business division of organization with which subscriber is affiliated, t = subscriber’s job title in organization with which it is affiliated”	o = “name of organization with which subscriber is affiliated” OID.2.5.4.97 = “organization identifier of organization with which subscriber is affiliated” s = “address (state) of organization with which subscriber is affiliated” l = “address (locality, street) of organization with which subscriber is affiliated” ou = business division of organization with which subscriber is affiliated t = subscriber’s job title in organization with which it is affiliated
cRLDistributionPoints (extnId: == 2 5 29 31, critical: == FALSE)		**Value**

cRLDistributionPoints DistributionPoint uniformResourceIdentifie	CRL distribution points CRL distribution points URI Type: OctetString Value: http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl
subjectKeyIdentifier (extnId: == 2 5 29 14, critical: == FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Information related to public key of certificate subject Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of subject	*Hash value of subjectPublicKey of subject

■CRL

(Standard Area)

Version		**Value**
Version	Version of certificate format Type: INTEGER Value: 1	 1 (Ver.2)
Signature		**Value**
AlgorithmIdentifier algorithm parameters	Identifier of cryptographic algorithm used for signing CRL (public key cryptography and hash function) Object ID of cryptographic algorithm (SHA-256) Type: OID Value: 1 2 840 113549 1 1 11 Parameters of cryptographic algorithm Type: NULL Value:	 1.2.840.113549.1.1.11 NULL
Issuer		**Value**
CountryName type value OrganizationIdentifer type value OrganizationName type value CommonName type value 	Country name of CRL issuer Object ID of country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization identifier of CRL issuer Object ID of organization identifier Type: OID Value: 2.5.4.97 Value of organization identifier Type: PrintableString Value: JCN3010401064771 Organization name of CRL issuer Object ID of organization name Type: OID Value: 2 5 4 10 Value of organization name Type: UTF8String Value: Cybertrust Japan Co., Ltd. Common name of CRL issuer Object ID of common name Type: OID Value: 2 5 4 3 Value of common name Type: UTF8String Value: Cybertrust iTrust Signature Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Signature Certification Authority
ThisUpdate		**Value**
ThisUpdate	Issue date of CRL Type: UTCTime Value: yymmddhhmmssZ	 *Commencement date of valid term
NextUpdate		**Value**
NextUpdate	Next scheduled update of CRL Type: UTCTime Value: yymmddhhmmssZ	 *Scheduled update

(Expansion Area)

authorityKeyIdentifier (extnId: == 2 5 29 35, critical: == FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Information related to public key of CRL issuer Identifier of public key Type: OctetString Value: Hash value of subjectPublicKey of issuer	 e9 53 9f 51 b0 1e 13 38 ac 7b 6c 28 05 e0 47 52 49 ef ba ce
cRLNumber (extnId: == 2 5 29 20, critical: == FALSE)		**Value**
cRLNumber	Sequence number of revocation list Type: INTEGER	

	Value: Unique integer	*CRL number

(Entry Area)

RevokedCertificates		**Value**
CertificateSerialNumber	Certificate serial number Type: INTEGER Value: Unique integer	*Serial number of revoked certificate
revocationDate	Revocation processing date Type: UTCTime Value: yymmddhhmmssZ	*Revocation processing date

(Entry Expansion Area)

invalidityDate (extnId: == 2 5 29 24, critical: == FALSE)		**Value**
invalidityDate	Invalidity date Type: GeneralizedTime Value: yyyymmddhhmmssZ	*Revocation processing date of certificate
cRLReason (extnId: == 2 5 29 21, critical: == FALSE)		**Value**
cRLReason	Revocation reason code Type: Enumerated Value: Revocation reason code	*Value of revocation reason code