JCSI Root CA

Certification Practice Statement

Version 2.6

English Version

Cybertrust Japan Co., Ltd.

June 30, 2021

Revision History

Version	Date	Reason for Revision
1.0	June 30, 2014	▪ Launch of JCSI Root CA, Formulation of Initial Version
1.1	March 30, 2017	▪ Made changes pursuant to the Baseline Requirements
1.2	July 20, 2017	▪ Made changes pursuant to the Baseline Requirements
1.3	February 21, 2018	▪ Made changes pursuant to the Baseline Requirements v1.5.6
1.4	April 23, 2018	▪ Correction of errors
1.5	June 1, 2018	▪ Remove "(iv) Other Method of Confirmation" from Section "3.2.2.5 Authentication for an IP Address"
1.6	September 5, 2018	▪ Made changes pursuant to “the JCSI certificate issuing service” ▪ Changed Address in "1.5.2 Contact Point" with headquarter shift ▪ Made changes pursuant to the Baseline Requirements
2.0	December 25, 2018	▪ Made changes pursuant to the “JCSI certificate issuing service” ▪ Made changes pursuant to the certificate profile of public and active intermediate CA ▪ Made changes pursuant to the Baseline Requirements ▪ Changed Repository URL from cybertrust.ne.jp to cybertrust.co.jp ▪ Correction of errors
2.1	May 10, 2019	▪ Made changes pursuant to the Baseline Requirements v1.6.5 ▪ Correction of errors
2.2	January 31, 2020	▪ Made changes pursuant to the Mozilla Root Store Policy v2.7 ▪ Made changes pursuant to the Baseline Requirements v1.6.7 ▪ Correction of errors
2.3	May 26, 2020	▪ Made changes pursuant to the Baseline Requirements v1.6.8 as follows ▪ Added not to issue certificates containing ".onion" in "3.2.2.4 Validation of Domain Authorization or Control" ▪ This Certification Authority ceases using the validation method listed in “3.2.2.4.6 Consistent website change” and starts using “3.2.2.4.18 Consistent website change” newly adopted, after the revision of Baseline Requirements v1.6.8 is effective ▪ "6.3.2 Certificate Operational Periods and Key Pair Usage Periods" Corrected the validity period of the Subscriber Certificate
2.4	March 10, 2021	▪ Update the version number of RFC document referenced in "CAA Record (Certification Authority Authorization Record) Procedures" ▪ Clarify the descriptions on the relevant documents mentioned in “1.1 Overview” ▪ Add descriptions in Section "3.2.2.4 Validation of Domain Authorization or Control" ▪ Modify the description in "4.9.1.1 Reasons for Revoking a Subscriber Certificate" ▪ Modify the description listed in "5.4.1 Types of events recorded" for the clarification ▪ Modify the description in "5.4.3 Retention Period for Audit Log" ▪ Add generation of subscriber’s key pair in "6.1.1 Key Pair Generation" ▪ Add descriptions in Section " 6.1.5 Key Sizes". ▪ Modified the description in Section "7.1.2 Certificate Extensions" ▪ Add description in " 7.1.3 Algorithm Object Identifier" ▪ Add description in " 7.1.4 Name Forms" ▪ Add descriptions in Section "7.2 CRL Profile". ▪ Add descriptions in Section "7.3 OCSP Profile" ▪ Modify the description in "9.6.3 Subscriber Representations and Warranties" ▪ Add definitions of terminology in Appendix A ▪ Correction of errors
2.5	April 30, 2021	▪ Add descriptions on reuse of previous validation in Section ”3.2.2.4 Validation of Domain Authorization or Control”

		▪ Add a revocation reason in Section " 4.9.1.1.2 Reason of Revocation by this Certification Authority" ▪ Add instructions for the problem report regarding a private key compromise in Section " 4.9.12 Special Requirements Related to Key Compromise" ▪ Modify the description in " 7.1.2 Certificate Extensions" ▪ Minor modifications on phraseology and fix of typos.
2.6	June 30, 2021	▪ Modified the acceptable HTTP status code response allowed for redirects listed in "3.2.2.4.18 Agreed‑Upon Change to Website v2" ▪ Modify the instructions for the problem report regarding a private key compromise in Section " 4.9.12 Special Requirements Related to Key Compromise" ▪ Add generation of subscriber's key pair in "6.1.1 Key Pair Generation" ▪ Add definitions of terminology in Appendix A ▪ Minor modifications on phraseology and fix of typos.

*Note
This "JCSI Root CA Certification Practice Statement Version 2.6" of Cybertrust Japan Co., Ltd. basically describes the following matters. However, please note that the following is a reference translation, and the effective statement is the original statement in the Japanese language. Please kindly note that Cybertrust Japan Co., Ltd. does not guarantee the accuracy of this English translation in comparison to the original statement in the Japanese language, and will not be liable in any way for any inconsistency between this English translation and the original statement in the Japanese language. Cybertrust Japan Co., Ltd. may provide the revised English translation with the date of revision for the same version of Cybertrust Japan's "JCSI Root CA Certification Practice Statement" Upon disclosure of the new version of "JCSI Root CA Certification Practice Statement" by Cybertrust Japan Co., Ltd., please stop referring to/using this documentation. Your understanding on above mentioned conditions is requested prior to refer to this documentation.

Table of Contents

cybertrust

1. Introduction

1.1 Overview

Cybertrust Japan Co., Ltd. ("Cybertrust") operates the JCSI Root Certification Authority (the "Root CA").

The Root CA is a publicly trusted Root CA that is identified with the following Certification Authority name, serial number, effective period and other information, and Cybertrust started operating the Root CA from the following launch date.

Name of Certification Authority	SecureSign RootCA11
Launch Date of Certification Authority	June 30, 2014
Serial Number of Certification Authority Certificate	01
Validity Period of Certification Authority Certificate	April 8, 2009 to April 8, 2029
Signature Algorithm	SHA1 with RSA
Key Length of Certification Authority	2048 bit
Hash value (SHA-1)	3BC49F48F8F373A09C1E BDF85BB1C365C7D811B3
Hash value (SHA-256)	BF0FEEFB9E3A581AD5F9 E9DB7589985743D26108 5C4D314F6F5D7259AA42 1612

Note that the key pair and root certificate of the Root CA were created on April 8, 2009 by Japan Certification Services, Inc.(*) ("JCSI"), and were acquired by Cybertrust after JCSI terminated the provision of its services using the foregoing the Root CA Certificate in 2014. With regard to JCSI's services and contents that were provided based on such services (including, but not limited to, certificates issued before June 30, 2014 to be chained to the foregoing the Root CA Certificate and revocation information, and related materials, contracts, and correspondences), JCSI was liable for such services and contents, and the Cybertrust has no knowledge of the same and is not liable therefor. Cybertrust is not JCSI's agent, trustee or any other representative.

(*) JCSI became a corporation in liquidation as of June 30, 2013. As of May 2014, JCSI's head office was located at Akasaka No. 1 Bldg. 4F, 4-9-17 Akasaka, Minato-ku, Tokyo 107-0052. After then, JCSI was completely liquidated as of February 26, 2015 and terminated as company.

The Root CA issues certificates (the “Subordinate CA Certificate”) of a JCSI Subordinate CA (the "Subordinate CA"; and the entity operating the Subordinate CA is hereinafter referred to as the "Subordinate CA Operator") that issues JCSI SSL/TLS certificates to subscribers, where JCSI SSL/TLS Certificate is an SSL/TLS server certificate (the “Subscriber Certificate”) for use in certifying servers and network devices upon performing SSL/TLS communication. As set forth in List of Definition, Subordinate CA is provided to the Subordinate CA Operator as the “JCSI certificate issuing service” (“this service”); and the Subordinate CA Operator is the same organization with Subscribers due to the characteristics of this service.

With the approval of Root CA Supervisor, the Root CA issues an OCSP server certificate that appends the digital signature to OCSP responses when the Root CA provides revocation information with regards to the Subordinate CA based on OCSP.

Furthermore, with the approval of Subordinate CA Supervisor, the Subordinate CA issues an OCSP server certificate that appends the digital signature to OCSP responses when the Subordinate CA provides revocation information with regards to the Subscriber Certificates based on OCSP.

The Root CA and the Subordinate CA (unless separately provided for herein, collectively, the “Certification Authorities”) are based on the following statement and laws and ordinances:

i. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates provided by CA/Browser Forum (“BR”)

ii. Network and Certificate System Security Requirements

iii. Requirements imposed also on certificate authorities by the provider of the browser in which the certificate of the root certificate authority is registered

- Microsoft Trusted Root Store (Program Requirements)
- Mozilla Root Store Policy
- Apple Root Store Program
- Chromium Root Store Policy

iv. this CPS; and

v. laws of Japan that are applicable to the operations to be performed by the Certification Authority established in Japan.

The Certification Authorities complies with the latest version of the BR. If any inconsistency exists between this CPS and the BR, the BR have precedence of this CPS.

This CPS prescribes the operation of the Root CA on and after the launch date as well as the various requirements pertaining thereto, the operation of the Subordinate CA as well as the various requirements pertaining thereto, and the requirements for the Subordinate CA to issue certificates. The requirements include obligations of the Certification Authorities, obligations of the subscribers, and obligations of the Relying Parties.

Upon specifying the various requirements in this CPS, the RFC3647 "Certificate Policy and Certification Practices Framework" set forth by the IETF PKIX Working Group shall be adopted. RFC3647 is an international guideline that sets forth the framework of CPS or CP. This CPS includes all material required by RFC 3647. Matters that do not apply to the Certification Authorities in the respective provisions of this CPS are indicated as "Not applicable".

The Subordinate CA does not individually prescribe a policy for each Subscriber Certificate ("CP"), and this CPS shall include the respective CPs. For clarification, this CPS applies to all the Certification Authorities including and under the JCSI Root Certification Authority.

1.2 Document Name and Identification

The official name of this CPS shall be the "JCSI Root CA Certification Practice Statement".

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

OID	Object
1.2.392.00200081.1.10.10	Cybertrust Japan JCSI Root 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 Root CA and Subordinate CA set forth in "1.1 Overview" of this CPS. The Certification Authority is composed from an Issuing Authority and a Registration Authority. The Certification Authority shall be governed by the Certification Authority Supervisor set forth in "5.2.1 Trusted Roles" of this CPS, and Cybertrust Japan Policy Authority ("CTJ PA") approves this CPS.

1.3.2 Registration Authority

The Registration Authority (“RA”) of the Root CA is operated by Cybertrust, and accepts applications for this service, and screens the applications based on this CPS. Based on the screening results, the Registration Authority instructs the Issuing Authority of the Root CA to issue, revoke the Subordinate CA Certificate, or dismiss the applications. Cybertrust does not delegate its RA operation to any of third parties.

The RA of the Subordinate CA is operated by the same organization with the Subscriber, and accepts applications for certificates from subscriber, and screens the applications based on this CPS. Based on the screening results, the Registration Authority instructs the Issuing Authority of the Subordinate CA to issue or revoke the Subscriber Certificate, or dismisses the applications. Cybertrust does not allow the Subordinate CA Operator to delegate its RA operation to any of third parties.

1.3.3 Issuing Authority

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

The Issuing Authority of the Subordinate CA is provided by Cybertrust in this service, and issues or revokes Subscriber Certificates based on instructions from the Registration Authority of the Subordinate CA. The Issuing Authority also controls the private key of the Subordinate CA based on this CPS.

1.3.4 Subscribers

A subscriber is an organization that applies for a certificate with the Subordinate CA and uses the Subscriber Certificate based on this CPS and the Subscriber Agreement.

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

Persons affiliated with the subscriber who may apply for a certificate with the Subordinate CA 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 the subscriber's organization.

1.3.5 Relying Parties

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

1.3.6 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Types of Certificates

1.4.1.1 Root CA Certificate

The certificate shown in Appendix B of this CPS is a Root CA certificate.

1.4.1.2 Subordinate CA Certificate

A Subordinate CA Certificate is the certificate of the Subordinate CA issued under the Root CA in this service.

Upon issuing a Subordinate CA Certificate, the Registration Authority of the Root CA shall screen the following matters based on this CPS:

i. legal or physical existence of subscribers and the appropriate value of Distinguished Name ("DN") is applied;

ii. a subscriber has the right to use the Fully-Qualified Domain Name ("FQDN") assigned in the permitted DNS Name of the NameConstraints extension in the Subordinate CA Certificate;

iii. employment of an application supervisor;

iv. acceptance of the Subscriber Agreement;

v. approval of the application supervisor for the procedural manager to submit an application; and

vi. high risk status, etc.*

*The following will be surveyed as the high-risk status, etc.:

- past phishing cases; and
- records of applications that were dismissed or records of Subordinate CA Certificates that were revoked by the Root CA in the past due to suspicion of fishing and other fraudulent acts (if present).

If there is suspicion based on the foregoing survey, the Root CA shall perform additional screening that it deems appropriate as needed.

1.4.1.3 Subscriber Certificates

The Subordinate CA issues a Certificate to subscribers.

The Subscriber Certificate certifies a subscriber's server or network device and realizes the SSL/TLS encrypted communication between such server or network device and a Relying Party's client device. Upon issuing a Subscriber Certificate, the Registration Authority of the Subordinate CA shall screen the following matters based on this CPS when the Subscriber Agreement is continued and active (subscriber uses this service continuously):

i. legal or physical existence of subscribers;

ii. a subscriber has the right to use the Fully-Qualified Domain Name ("FQDN") included in the Subscriber Certificate and shall not conflict with the NameConstraints;

iii. employment of an application supervisor;

iv. approval of the application supervisor for the procedural manager to submit an application; and

v. high risk status, etc.*

*The following or additional verification as reasonably necessary will be surveyed as the high-risk status:

- past fishing cases; and
- records of applications that were dismissed or records of the Subscriber Certificates that were revoked by the Subordinate CA in the past due to suspicion of fishing and other fraudulent acts.

If there is suspicion of fraudulent use of a certificate for which an application was submitted with the Subordinate CA based on the foregoing survey, the Subordinate CA shall perform additional screening that it deems appropriate as needed.

Note that the Subscriber Certificate shall be include no OU in this service.

And no EV SSL/TLS certificate is issued under the Root CA.

1.4.1.4 OCSP Server Certificate

OCSP server certificate is a certificate for OCSP response that the Certification Authorities issue and use. OCSP server certificate appends the digital signature to OCSP responses when the Certification Authority provides revocation information with regard to the Certification Authority based on OCSP.

1.4.2 Appropriate Certificate Uses

Uses of a certificate shall be as set forth below.

1.4.2.1 Subscriber Certificate

i. Certification of devices (server, network device, etc.) in which the Certificate is to be used

ii. SSL or TLS encrypted communication

1.4.2.2 OCSP Server Certificate

i. Digital signing to OCSP responses providing revocation information

1.4.2.3 Subordinate CA Certificate

ii. Issuing a Subscriber Certificate to Subscriber who owns a domain name set forth in NameConstraints

iii. Issuing an OCSP Server Certificate which is for the OCSP responder providing revocation information of the Subscriber Certificates

1.4.3 Prohibited Certificate Uses

The use of certificates for any purpose other than as set forth in "1.4.2 Appropriate Certificate Uses" of this CPS shall be prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Documents

This CPS and the Subscriber Agreement are controlled by the CTJ PA.

1.5.2 Contact Persons

The inquiries related to this CPS and other related matters are accepted at the following contact information.

This contact point is specified in the repositories and it shall be indicated that the inquiries are accepted 24 hours a day, 365 days a year.

Contact Information
Cybertrust Japan Co., Ltd., JCSI Root Support Address: ARK Hills Sengokuyama Mori Tower 35F, 1-9-10 Roppongi, Minato-ku, Tokyo 106-0032 Email Address: jcsi-r@cybertrust.ne.jp Inquiries and complaints: ・Inquiries regarding the application process for issuance and technical inquiries ・Inquiries regarding revocation requests and application process ・Inquiries regarding problems with certificates or upon discovery of fraudulent certificates ・Communication of other complaints ・Other inquiries regarding this CPS, etc.

1.5.3 Person Determining CPS Suitability for the Policy

Cybertrust determines the suitability of this CPS.

1.5.4 CPS Approval Procedures

The suitability of this CPS is approved by the CTJ PA during the assessment/approval procedures set forth in Cybertrust's internal rules and regulations.

1.6 Definitions and Acronyms

As prescribed in Appendix A of this CPS.

2. Publication and Repository Responsibilities

2.1 Repositories

Repositories are operated by Cybertrust. Cybertrust updates this CPS when necessary or at least annually.

2.2 Publication of Information

The repositories are published as follows.

i. Publish the following information on https://www.cybertrust.co.jp/jcsi/repository.html

- this CPS

Note that the Subscriber Agreement is disclosed to the applicant of this service by the JCSI Root Support.

ii. Publish the following information on http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt

- Root CA Certificate

iii. Publish the following information on http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/cdp.crl

- CRL issued by the Root CA

2.3 Time or Frequency of Publication

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

i. this repository shall be maintained available in public 24 hours a day, 365 days a year;

ii. this CPS shall be published each time it is amended;

iii. the CRL shall be updated as prescribed in "4.9.7 CRL Issuance Frequency" of this CPS and the published; and

iv. the Root CA Certificate shall be published at least during the operation period of this Root CA.

2.4 Access Control on Repositories

The Certification Authorities make its repositories publicly available in a read-only manner.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Subscribers are 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 shall have the meaning of the subsequent paragraph.

DN Item	Meaning
Common Name	Name of Subordinate CA, or complete host name of server or network device to use the Subscriber Certificate
Organization	Name of organization of the Subscriber
Organization Unit	(Usage prohibited in this service.)
Locality	Address of business location of the Subscriber (locality)
State or Province	Address of business location of the Subscriber (state or province)
Country	Address of business location of the Subscriber (country)

3.1.3 Anonymity or Pseudonymity of Subscribers

The Certification Authorities do not accept any certificate request by anonymity or pseudonymity of subscriber.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

The Certification Authorities do not authenticate the copyrights, trade secrets, trademark rights, utility model rights, patent rights and other intellectual property rights (including, but not limited to, rights for obtaining patents and other intellectual properties; simply "Intellectual Property Rights") upon issuing a certificate.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

A certificate signing request ("CSR") which constitutes a part of the application information from a subscriber includes a digital signature encrypted with a public key and a private key corresponding to the public key.

The Subordinate CA verifies the digital signature by using the public key included in the CSR and thereby validates that the digital signature was signed using the subscriber's private key and determines that the subscriber is in possession of the private key.

Based on the usage of this service, the Root CA shall deem that the Subordinate CA Operator has become the Manager of Subordinate CA’s private key.

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Identity

The Certification Authorities shall screen and verify the matters set forth in “1.4.1 Types of Certificates” of this CPS.

Upon verifying the subscriber, the Certification Authorities shall use public documents and data, documents and data provided by a third party that is deemed reliable by the Certification Authorities, or documents and data provided by the subscriber, as well as make inquiries to an appropriate individual affiliated with the subscriber or the organization configuring the subscriber. Moreover, the Certification Authorities shall visit the subscriber and conduct an on-site survey as needed.

However, when there are documents or data that had been received from the subscriber or documents or data that had been independently obtained by the Certification Authorities during the period notified to the subscriber, and such documents or data have been screened successfully by the Certification Authorities, the Certification Authorities shall not request the resubmission of such documents or data.

Details regarding the verification procedures to be requested to subscribers shall be notified individually to the subscribers.

Note that it shall not be allowed for the subscriber to get and use a Certificate with a domain name owned by a third party other than the subscriber in this service.

3.2.2.2 DBA/Tradename

The Certification Authorities do not allow DBA/Tradename to be included in the Subscriber Certificate.

3.2.2.3 Verification of Country

The Certification Authorities confirm the Country included in the Subscriber Certificate with this CPS "3.2.2.1 Identity".

3.2.2.4 Validation of Domain Authorization or Control

The Root CA shall confirm that prior to issuance the Subordinate CA Certificate, the Root CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Subordinate CA Certificates via dNSNames in permittedSubtrees within the NameConstraints extension using at least one of the methods listed below.

The Subordinate CA shall confirm that prior to issuance the Certificate, the Subordinate CA has validated each Fully-Qualified Domain Name (FQDN) listed in Subscriber Certificates using dNSNames in the subjectAltName extension using at least one of the methods listed below. The Certification Authorities does not issue a certificate for a FQDN contains ".onion" as the rightmost label.

Validation results on the subscriber’s authorization or control of the domain name may be reused for less than 398 days from the day the initial validation completes to issue multiple Certificates. The Certification Authority shall again verify the authorization or control of the domain name for the certificate request if the previous validation results are expired. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of BR) prior to Subscriber Certificate issuance. For purposes of domain validation, the term Applicant include the Applicant's Parent Company, Subsidiary Company, or Affiliate.

The Certification Authorities shall maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the NameConstraints extension.

And the Certification Authorities shall not delegate the validation of the domain names to any third party.

3.2.2.4.1 Validating the Applicant as a Domain Contact

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.1.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

The Certification Authorities shall confirm the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail may confirm control of multiple Authorization Domain Names.

The Certification Authorities may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

The Certification Authorities may resend the email, fax, SMS, or postal mail in its entirety, including reuse of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the Subordinate CA may also issue the Subscriber Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Certification Authorities shall not perform validations using this method set forth below after May 31, 2019. Completed validations using this method shall continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

The Certification Authorities shall confirm the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The Certification Authorities must place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call shall be made to a single number and may confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Note: Once the FQDN has been validated using this method, the Subordinate CA may also issue the Subscriber Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

The Certification Authorities shall confirm the Applicant's control over the FQDN by

i. sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'host master', or 'postmaster' as the local part, followed by the at sign ("@"), followed by an Authorization Domain Name,
ii. including a Random Value in the email, and
iii. receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the reuse of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the Subordinate CA may also issue the Subscriber Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.5.

3.2.2.4.6 Agreed-Upon Change to Website

The Certification Authorities SHALL NOT perform screening using this method after June 1, 2020. However, completed validations using this method before the date SHALL continue to be valid during the applicable certificate data reuse periods.

The Certification Authority shall confirm the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the Certification Authorities via HTTP/HTTPS over an Authorized Port:

i. The presence of Required Website Content contained in the content of a file. The entire Required Website Content must not appear in the request used to retrieve the file or web page, or

ii. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value must not appear in the request.

If a Random Value is used, the Certification Authority shall provide a Random Value unique to the Subscriber Certificate request and shall not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certification Authority request, the timeframe permitted for reuse of validated information relevant to the Certification Authority (such as in BR 4.2.1).

However, the Subordinate CA with nameConstraints shall not adopt Request Token.

3.2.2.4.7 DNS Change

The Certification Authorities shall confirm the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the Certification Authorities shall provide a Random Value unique to the Certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in BR 4.2.1).

However, the Subordinate CA with nameConstraints shall not adopt Request Token.

3.2.2.4.8 IP Address

The Root CA does not allow to issue the Subscriber Certificate with an IPAddress under the Root CA and it specifies excludedSubtrees of any IP addresses within the NameConstraints extension in the Subordinate CA Certificate.

3.2.2.4.9 Test Certificate

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.9.

3.2.2.4.10 TLS Using a Random Number

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.10.

3.2.2.4.11 Any Other Method

The Certification Authorities shall not use this method set forth in BR 3.2.2.4.11.

3.2.2.4.12 Validating Applicant as a Domain Contact

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.12.

3.2.2.4.13 Email to DNS CAA Contact

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.13.

3.2.2.4.14 Email to DNS TXT Contact

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.14.

3.2.2.4.15 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the Authorization Domain Name. Each phone call may confirm control of multiple Authorization Domain Names provided that the same Domain Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name. In the event that someone other than a Domain Contact is reached, the Certification Authorities may request to be transferred to the Domain Contact. In the event of reaching voicemail, the Certification Authorities may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value must be returned to the Certification Authorities to approve the request. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the Subordinate CA may also issue the Subscriber Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the Authorization Domain Name. Each phone call may confirm control of multiple Authorization Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each Authorization Domain Name being verified and they provide a confirming response for each Authorization Domain Name. The Certification Authorities may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, the Certification Authorities may leave the Random Value and the Authorization Domain Name(s) being validated. The Random Value must be returned to the Certification Authorities to approve the request. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the Subordinate CA may also issue the Subscriber Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.17.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

i. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and

ii. The Certification Authorities MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

i. MUST be located on the Authorization Domain Name, and

ii. MUST be located under the "/.well-known/pki-validation" directory, and

iii. MUST be retrieved via either the "http" or "https" scheme, and

iv. MUST be accessed over an Authorized Port.

If the Certification Authorities follows redirects the following apply:

i. Redirects MUST be initiated at the HTTP protocol layer.

Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

ii. Redirects MUST be to resource URLs with either via the "http" or "https" scheme.

iii. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

i. The Certification Authorities MUST provide a Random Value unique to the certificate request.

ii. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation.

However, the Subordinate CA with nameConstraints shall not adopt Request Token.

Note: Once the FQDN has been validated using this method, the Subordinate CA may also issue the Subscriber Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.19.

3.2.2.4.20 TLS Using ALPN

The Certification Authorities do not adopt this method set forth in BR 3.2.2.4.20.

3.2.2.5 Authentication for an IP Address

The Root CA does not allow to issue the Subscriber Certificate with an IPAddress under the Root CA and it specifies excludedSubtrees of any IP addresses within the NameConstraints extension in the Subordinate CA Certificate.

3.2.2.6 Wildcard Domain Validation

Before issuing a Subscriber Certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the Subordinate CA must determine if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation). Determination of registry control shall follow practices as set forth in BR 3.2.2.6.

If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, the Subordinate CA must refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. Certification Authorities MUST NOT issue “*.co.uk” or “*.local”, but MAY issue “*.example.com” to Example Co.).

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the Certification Authorities shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The Certification Authorities consider the following during its evaluation:

i. The age of the information provided,

ii. The frequency of updates to the information source,

iii. The data provider and purpose of the data collection,

iv. The public accessibility of the data availability, and

v. The relative difficulty in falsifying or altering the data.

Databases maintained by the Certification Authorities, 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.

3.2.2.8 CAA Record (Certification Authority Authorization Record) Procedures

The Root CA shall deem that a subscriber has designated the Subordinate CA, the Technically Constrained Subordinate CA, as a certificate authority that permits issuances of Subscriber Certificates when the subscriber submits this service to be provided the Subordinate CA. And the Root CA shall not verify the CAA Record when the Root CA issues the Subordinate CA Certificate. Similarly, the Subordinate CA does not verify the CAA Record since the CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA as set forth in BR 3.2.2.8.

Note that the Subordinate CA which is not Technically Constrained will verify the CAA Record set forth in RFC 8659(DNS Certification Authority Authorization (CAA) Resource Record) in accordance with the BR 3.2.2.8. If the CAA record (issue / issuewild) contains any values set forth in "4.2.1 Performing Identification and Authentication Functions" of this CPS, this Subordinate CA recognizes that it is designated as a certificate authority that permits issuances of the certificates.

3.2.3 Authentication of Individual Identity

The Subordinate CA shall not issue a certificate to an individual.

3.2.4 Non-verified Subscriber Information

Not applicable.

3.2.5 Verification of Authority

The Certification Authorities shall verify the employment of the application supervisor and the authority to submit an application on behalf of the subscriber. The Certification Authorities 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 call-back or means equivalent to call-back. The phone number to be used for the call-back 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 Authorities.

3.2.6 Criteria for Interoperation or Certification

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The provisions of "3.2 Initial Identity Validation" of this CPS shall apply correspondingly.

3.3.2 Identification and Authentication for Re-Key after Revocation

To be performed based on the same procedures as "3.2 Initial Identity Validation" of this CPS.

However, when it is verified that the public key, certification information and expiration date included in the CSR of the re-issuance application coincide with the certificate of the re-issuer, verification based on "3.2 Initial Identity Validation" of this CPS will not be performed, and a certificate shall be issued based on the verification of the foregoing coincidence.

3.4 Identification and Authentication for Revocation Request

When the Subordinate CA receives a revocation request from a subscriber via email, the Subordinate CA 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 Subordinate CA shall compare the information notified to the Subordinate CA upon application for issuance of a Subscriber Certificate and the information only known to the Subordinate CA 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 survey the reason of revocation and verify with the subscriber.

When the reason for revocation in the revocation request from a subscriber or a party other than that subscriber corresponds to a revocation event set forth in the Subscriber Agreement of the Certificate, the Certification Authority shall revoke the Certificate upon notifying the subscriber.

The email address to be used for the revocation request is indicated in "1.5.2 Contact Persons" and Cybertrust's website.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Persons who may apply with the Certification Authorities shall only be the application supervisor, or a procedural manager who was authorized by the application to supervisor submit an application.

Appointment of the application supervisor or the procedural manager shall be pursuant to the provisions of "1.3.4 Subscribers" of this CPS.

The Certification Authorities' verification of a subscriber's intent to submit an application shall be confirmed by the application supervisor or a person affiliated with the subscriber who was authorized by the application supervisor.

4.1.2 Enrolment Process and Responsibilities

A subscriber shall apply for this service upon accepting this CPS and the Subscriber Agreement. Upon filing an application, a subscriber is responsible for providing true and accurate information. The method of applying for this service shall be notified individually to the subscribers.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

To be performed by the Registration Authority of the Certification Authorities based on the same procedures as "3.2 Initial Identity Validation" of this CPS.

If the CAA record (issue/issuewild) contains any of the following values, this Subordinate CA recognizes that it is designated as a certificate authority that permits issuances of the certificates.

cybertrust.ne.jp

jcsinc.co.jp

4.2.2 Approval or Rejection of Certificate Application

When all requirements prescribed in "3.2 Initial Identity Validation" of this CPS are confirmed, the Registration Authority of the Certification Authorities shall approve the application, and instruct the Issuing Authority to issue a certificate. The Certification Authorities shall never 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 Authorities shall dismiss the application for issuing a certificate, and reject issuance. In the foregoing case, the Certification Authorities shall notify the reason of such rejection to the application supervisor or the procedural manager who submitted the application. The Certification Authorities shall not return the information and data obtained from the application supervisor or the procedural manager during the application process.

When the application supervisor or the procedural manager withdraws the submitted application, the Certification Authorities shall dismiss such application. The Certification Authorities shall not return the information and data obtained from the application supervisor or the procedural manager during the application process.

Note that the Certification Authorities shall not issue certificates containing Internal Names.

4.2.3 Time to Process Certificate Applications

After the Registration Authority of the Certification Authorities processes the application based on the provisions of "4.2 Certificate Application Processing" of this CPS, the Issuing Authority shall issue a Certificate without delay.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

After completing the application procedures based on "3.2 Initial Identity Validation" of this CPS, the Registration Authority of the Certification Authorities shall instruct the Issuing Authority to issue the certificate. Simultaneously with issuing the certificate, the Issuing Authority shall send to the subscriber the notice.

4.3.2 Notification of Certificate Issuance

Promptly after the certificate is issued, the Certification Authorities shall send to the subscriber the notice, and the procedures required for the subscriber to accept the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct constituting Certificate Acceptance

A subscriber shall accept a Certificate according to the email sent from the Subordinate CA based on the provisions of "4.3.2 Notification of Certificate Issuance" of this CPS. The Subordinate CA shall deem that a subscriber has accepted the certificate when the email is sent to the subscriber.

4.4.2 Publication of the Certificate by Certification Authority

The Subordinate CA basically does not publish a Subscriber Certificate. However, the Subordinate CA may register and publish the Subscriber Certificates to CT log server, CCADB and so on.

4.4.3 Notification of Certificate Issuance of by Certification Authority to Other Entities

The Subordinate CA shall not notify the issuance of the Certificate to other participants based on "4.3.2 Notification of Certificate Issuance" 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 the Certificate only for the usage set forth in "1.4.2 Appropriate Certificate Uses" of this CPS, and use for any other usage is not allowed. Moreover, a subscriber's private key and the Certificate may 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 the 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 "1.4.2 Appropriate Certificate Uses" of this CPS.

Other obligations of a Relying Party regarding the use of a subscriber's public key and the Certificate are set forth in "9.6.4 Relying Party Representations and Warranties".

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

The Subordinate CA shall accept a renewal request pursuant to the expiration of the valid term of the Subscriber Certificate.

4.6.2 Who May Request Renewal

The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CPS shall apply correspondingly.

4.6.3 Processing Certificate Renewal Requests

The provisions of "4.2 Certificate Application Processing" of this CPS shall apply correspondingly.

4.6.4 Notification of New Certificate Issuance to Subscriber

The provisions of "4.3.2 Notification of Certificate Issuance" of this CPS shall apply correspondingly.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The provisions of "4.4.1 Conduct constituting Certificate Acceptance" of this CPS shall apply correspondingly.

4.6.6 Publication of the Renewal Certificate by Certification Authority

The provisions of "4.4.2 Publication of the Certificate by Certification Authority" of this CPS shall apply correspondingly.

4.6.7 Notification of Certificate Issuance by Certification Authority to Other Entities

The provisions of "4.4.3 Notification of Certificate Issuance of by Certification Authority to Other Entities" of this CPS shall apply correspondingly.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

The Subordinate CA shall accept a renewal request pursuant to the expiration of the valid term of the Certificate used by a subscriber.

4.7.2 Who May Request Certification of a new Public Key

The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CPS shall apply correspondingly.

4.7.3 Processing certificate Re-Key Requests

The provisions of "4.2 Certificate Application Processing" of this CPS shall apply correspondingly.

4.7.4 Notification of new certificate Issuance to Subscriber

The provisions of "4.3.2 Notification of Certificate Issuance" of this CPS shall apply correspondingly.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The provisions of "4.4.1 Conduct constituting Certificate Acceptance" of this CPS shall apply correspondingly.

4.7.6 Publication of the Re-Keyed Certificate by Certification Authority

The provisions of "4.4.2Publication of the Certificate by Certification Authority" of this CPS shall apply correspondingly.

4.7.7 Notification of Certificate Issuance by Certification Authority to Other Entities

The provisions of "4.4.3 Notification of Certificate Issuance of by Certification Authority to Other Entities" of this CPS shall apply correspondingly.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

The Subordinate CA shall not accept a request for modifying a previously issued Subscriber Certificate.

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

Not applicable.

4.8.7 Notification of Certificate Issuance by Certification Authority to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstance for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

4.9.1.1.1 Reason of Revocation by Subscriber

In the occurrence of any one of the following events, a subscriber must submit a request to the Subordinate CA for revoking the corresponding Subscriber Certificate:

i. a subscriber discovers a Subscriber 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 misuse or unauthorized use of its private key or the Certificate or the possibility thereof;

iv. there is modification to the contents of a Subscriber Certificate;

v. a subscriber loses its right to exclusively use the FQDN included in the Subscriber Certificate;

vi. a subscriber learns the subject information listed in subscriber’s certificate is no longer accurate;

vii. a subscriber violates one or more of its material obligations under this CPS or the Subscriber Agreement;

viii. a subscriber discovers that the certificate was not issued in accordance with the relevant requirements of CA/Browser Forum, this CPS, or the Subscriber Agreement;

ix. a subscriber discovers any values in conflict with the NameConstraints are included in the Subscriber Certificate;

x. a subscriber discovers the Subscriber Certificate includes the organization unit (OU); or

iv. a subscriber wishes to cancel the Subscriber Agreement.

4.9.1.1.2 Reason of Revocation by the Subordinate CA

Prior to revoking a Subscriber Certificate, the Subordinate CA verifies the identity and authority of the entity requesting revocation. The Subordinate CA will revoke a Certificate within 24 hours if one or more of the following occurs:

i. The Subscriber requests in writing that the Subordinate CA revoke the Subscriber Certificate;

ii. The Subscriber notifies the Subordinate CA that the original Certificate request was not authorized and does not retroactively grant authorization;

iii. The Subordinate CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or

iv. The Subordinate CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

v. The Subordinate CA obtains evidence that the validation of domain authorization or control for any FDQN in the Certificate should not be relied upon.

The Subordinate CA may revoke a Subscriber Certificate within 24 hours and must revoke a Subscriber Certificate within 5 days if one or more of the following occurs:

i. The Subscriber Certificate no longer complies with the requirements of BR 6.1.5 and BR 6.1.6;

ii. Cybertrust obtains evidence that the Subscriber Certificate was misused;

iii. a subscriber breaches a material obligation under this CPS or the Subscriber Agreement;

iv. Cybertrust confirms any circumstance indicating that use of a FQDN in the Subscriber Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);

v. Cybertrust confirms that a subscriber's Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;

vi. Cybertrust confirms a material change in the information contained in the Subscriber Certificate;

vii. Cybertrust confirms that the Subscriber Certificate was not issued in accordance with the applicable requirements such as CA/Browser Forum requirements or this CPS;

viii. Cybertrust determines or confirms that, based on reasonable evidence, any of the information appearing in the Subscriber Certificate is inaccurate;

ix. The right of the Subordinate CA to issue the Subscriber Certificates under the CA/Browser Forum requirements expires, is revoked or is terminated, unless the Subordinate CA has made arrangements to continue maintaining the CRL/OCSP Repository;

x. Revocation is required by this CPS; or

xi. Cybertrust confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise.

The Subordinate CA may revoke any Subscriber Certificates in its sole discretion, including if one or more of the following occurs:

i. The revocation request is confirmed by "3.4 Identification and Authentication for Revocation Request" of this CP;

ii. Either the Subscriber's or Cybertrust's obligations under this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, information of this Certification Authority, the Subscriber, or the relying party is materially threatened or compromised;

iii. Cybertrust received a lawful and binding order from a government or regulatory body to revoke the Subscriber Certificate;

iv. The Subordinate CA ceased operations and did not arrange for another Certificate Authority to provide revocation support for the Certificates;

v. The technical content or format of the Subscriber Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

vi. The Subscriber was added as a denied party or prohibited person to a blacklist;

vii. a subscriber fails to pay the fee of the Certificate in breach of Cybertrust's prescribed billing conditions;

viii. Cybertrust cancels the Subscriber Agreement with a subscriber based on the Subscriber Agreement; or

ix. the Subordinate CA learns that the private key of the Subordinate CA and/or the Root CA has been compromised or there is a possibility thereof.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

In the occurrence of the following event, the Root CA shall revoke the corresponding Subordinate CA Certificate within seven (7) days at the time that such event is discovered:

i. The Subordinate CA requests revocation in writing;

ii. The Subordinate CA notifies the Root CA that the original application to this service was not authorized and does not retroactively grant authorization;

iii. The Root CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Subordinate CA Certificate suffered a Key Compromise or no longer complies with the requirements of BR 6.1.5 and BR 6.1.6;

iv. The Root CA obtains evidence that the Subordinate CA Certificate was misused;

v. The Root CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the BR or the CPS;

vi. The Root CA determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;

vii. The Root CA or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Subscriber Certificate;

viii. The Root CA's or the Subordinate CA's right under these Requirements expires or is revoked or terminated, unless they have made arrangements to continue maintaining the CRL/OCSP Repository;

ix. Revocation of the Subordinate CA Certificate is required by the Root CA's CPS;

x. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties; or

xi. Cybertrust terminates this service.

4.9.1.3 Reason of Revoking Other certificates

4.9.1.1.1 Root CA Certificate

In the occurrence of any one of the following events, the Root CA revokes the Root CA Certificate at the time that such event is discovered; provided, however, that, with regard to (ii) below, the Root CA may revoke its certificate on a day that is separately notified by the Root CA before termination of operations:

i. when it is learned that the private key of the Root CA has been compromised; or

ii. when the Root CA is to terminate its certification operations.

4.9.1.1.2 OCSP server Certificate

In the occurrence of any of the following events, the Certification Authorities revoke the corresponding OCSP server certificate at the time that such event is discovered:

i. when it is learned that the private key of an OCSP server certificate has been compromised; or

ii. when the Certification Authority is to terminate its certification operations.

4.9.2 Who Can Request Revocation

Persons who may request revocation shall be the application supervisor, the procedural manager.

4.9.3 Procedure for Revocation Request

A subscriber shall submit a revocation request basically by email. The revocation request must include reason of revocation, contact information and so on. The Certification Authorities shall verify the reason of revocation.

The revocation of the Certification Authority certificate and the OCSP certificate shall be instructed by the Certification Authority Supervisor to the Issuing Authority.

4.9.4 Revocation Request Grace Period

In the occurrence of an event corresponding to "4.9.1.1 Reasons for Revoking a Subscriber Certificate" of this CPS, the Subscriber shall promptly submit a revocation request.

In the occurrence of an event corresponding to "4.9.1.2 Reasons for Revoking a Subordinate CA Certificate" or "4.9.1.3 Reason of Revoking Other certificates" of this CPS, the Certification Authority Supervisor shall promptly give revocation instructions.

4.9.5 Time within which Certification Authority Must Process the Revocation Request

The Certification Authorities accept the revocation request 24/7.

Within 24 hours after receiving a Certificate Problem Report, the Certification Authorities shall investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report. After reviewing the facts and circumstances, the Certification Authorities shall work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the Certification Authorities will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation must not exceed the time frame set forth in Section4.9.1.1. The date selected by the Certification Authorities should consider the following criteria:

i. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);

ii. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);

iii. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

iv. The entity making the complaint; and

v. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

The Relying Parties shall confirm the certificate revocation of the Certificate with the CRLs issued by the Certification Authorities or the OCSP servers.

4.9.7 CRL Issuance Frequency

The Subordinate CA issues the CRL in a cycle of less than 24 hours.

The Root CA shall issue the CRL for each occurrence of an event corresponding to "4.9.1.2 Reasons for Revoking a Subordinate CA Certificate" or "4.9.1.3 Reason of Revoking Other certificates" of this CPS or once a year at least.

4.9.8 Maximum Latency for CRLs

The validity period of the Subordinate CA's CRL is 168 hours.

The Subordinate CA shall publish each CRLs in the repositories no later than one (1) hour after the issuance thereof.

4.9.9 On-Line Revocation/Status Checking Availability

OCSP responses conform to RFC 6960 and/or RFC5019.

OCSP responses is signed by the OCSP Responder whose Certificate is signed by the Certification Authority that issued the Certificate whose revocation status is being checked.

The OCSP signing Certificate contains the extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

The Certification Authorities shall provide revocation information based on OCSP, in addition to CRL.

The Certification Authorities support an OCSP capability using the GET method, as described in RFC6960 and/or RFC5019.

The Subordinate CA shall renew the OCSP response, which has a maximum expiration time of 168 hours, in a cycle of less than 96 hours.

The Root CA shall provide revocation information of the Subordinate CA Certificate based on OCSP. The Root CA shall update the OCSP response at least one a year, or no later than 24 hours after it revokes a Subordinate CA Certificate.

The responder shall not respond with a "good" status. if the OCSP responder receives a request for status of a certificate that has not been issued.

The Certification Authorities monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

The OCSP responder of the Root CA and the Subordinate CA do not provide definitive responses about "reserved" certificate serial numbers, since the CAs do not issue the Precertificate [RFC6962].

The URL to accept OCSP requests in regard to the Root CA shall be as follows;

http://rtocsp.managedpki.ne.jp/OcspServer

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

4.9.12.1 Certificate

When the Subordinate CA learns that the Subscriber’s private key has been compromised or there is a possibility thereof, the Subordinate CA shall take the revocation procedures of the Certificate based on "4.9.3 Procedure for Revocation Request" of this CPS. This Certification Authority accepts a report for the Private Key Compromise from the third party at the problem report contact listed in "1.5.2 Contact Persons" of this CP.

Reports or subsequent responses to this Certification Authority of key compromise shall include;

i. the demonstration on the Private Key Compromise:
   - private Key itself and/or
   - a CSR signed by the compromised private key with the Common Name of which value specified by this Certification Authority; and

ii. name and reachable contact information such as email address and/or phone number of a person who reports the problem.

4.9.12.2 OCSP Server Certificate

When the Certification Authority learns that the private key of an OCSP server certificate has been compromised, the Certification Authority shall take the revocation procedures of the corresponding OCSP server certificate based on "4.9.3 Procedure for Revocation Request of this CPS.

4.9.13 Circumstances for Suspension

The Certification Authorities do 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 Authorities shall not provide services that enable the verification of the certificate status other than by way of CRL and OCSP.

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP Response shall not be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

The Certification Authorities shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

The Certification Authorities shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the Certification Authorities.

The Certification Authorities shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities or CTJ PA, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

The reasons for ending the use of this service shall be set forth in the respective Subscriber Agreements. Moreover, if a subscriber wishes to terminate the Subscriber Agreement midway during the valid term of the certificate, the subscriber must submit a revocation request of the Subscriber Certificate with the Subordinate CA 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. Management, Operational, And Physical Controls

5.1 Physical Security 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 (the "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 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 24/7.

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 Medium Storage

Mediums containing the backup data of the Certification Authority system and forms and the like relating to the operation of the Certification Authority shall be stored 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 Authorities and important assets for system recovery shall be stored 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 Authorities shall set forth the personnel required for operating the Certification Authorities (the "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 (issuing an OCSP server certificate or like that based on Certification Authority Supervisor's instructions including) 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 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 Individuals Required per Task

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

5.2.3 Identification and Authentication for Trusted Role

The Certification Authorities 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 confirm and verify the identification and entrance/operation authority.

5.2.4 Roles Requiring Separation of Duties

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, Clearances 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 and Procedures

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

i. when this CPS is amended, and CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager or the Registration Authority Manager deems necessary;

ii. when the Certification Authority system is changed, and CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager or the Registration Authority Manager deems necessary; or

iii. 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 Authorities shall rotate jobs of the Certification Authority Staff as needed.

5.3.6 Sanction for Unauthorized Actions

When a Certification Authority Staff conducts an act that is in breach of this CPS, 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 Controls

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 Authorities 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 Authorities shall collect the following records as monitoring logs. The records shall include the date and time, identity of the person making the journal record, and description of the record.

i. The Certification Authority certificate and key lifecycle events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Certificate requests, renewal, and re-key requests, and revocation;
- Approval and rejection of certificate requests;
- Cryptographic device lifecycle management events;
- Generation of Certificate Revocation Lists and OCSP entries;
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

ii. Subscriber Certificate lifecycle management events, including:

- Certificate requests, renewal, and re-key requests, and revocation;
- All verification activities stipulated in the relevant requirements and the Certification Authority's Certification Practice Statement;
- Approval and rejection of certificate requests;
- Issuance of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries.

iii. Security events, including:

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- Installation, update and removal of software on a Certificate System;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the Certification Authority facility.

iv. Log records MUST include the following elements:

- Date and time of record;
- Identity of the person making the journal record; and
- Description of the record.

5.4.2 Frequency for Processing and Archiving Audit Logs

The Certification Authorities 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 Logs

The Certification Authority SHALL retain, for at least seven years:

i. Certification Authority certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1) of the BRs) after the later occurrence of:

- the destruction of the Certification Authority Private Key; or
- the revocation or expiration of the final Certification Authority Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the Certification Authority Private Key.

ii. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2) of the BRs) after the revocation or expiration of the Subscriber Certificate.

iii. Any security event records (as set forth in Section 5.4.1 (3) of the BRs) after the event occurred.

When the monitoring logs are no longer required, the Certification Authorities 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 Authorities shall implement access control the monitoring logs so that only authorized personnel can peruse the monitoring logs. The Certification Authorities 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 Authorities 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 Log Accumulation System

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 Authorities shall collect and inspect the monitoring log without notifying the party that caused the event.

5.4.8 Vulnerability Assessments

Cybertrust performs an annual risk assessment once a year that identifies and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of the Certification Authorities (The OCSP servers of the Certification Authorities including.). Cybertrust also routinely assesses the sufficiency of procedures, information systems, technology, and other arrangements that Cybertrust has in place to control such risks. Cybertrust's Internal Auditors review the security audit data checks. Cybertrust's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files and unauthenticated responses.

5.5 Records Archival

5.5.1 Types of Records Archived

The Certification Authorities shall archive the following information in addition to the monitoring logs prescribed in "5.4.1 Types of Events Recorded" of this CPS:

i. Certification Authority Certificate;

ii. Subscriber Certificate;

iii. CRL;

iv. internal audit report;

v. external audit report;

vi. application forms and data; and

vii. this CPS.

5.5.2 Retention Period for Archive

The Certification Authorities shall archive the records prescribed in "5.5.1 Types of Records Archived" of this CPS for at least 7 years beyond the effective period of the relevant certificate or during the operation period of the Certification Authorities, whichever comes first.

When records are no longer required, the Certification Authorities 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 Archive 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 Authorities 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. The Certification Authorities 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

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

5.6 Key Changeover

Not applicable.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

5.7.1.1 In the event of Compromise of the Subordinate CA

When the private key of the Subordinate CA is compromised in this service, Cybertrust shall execute the following, and simultaneously notify the fact of such compromise to subscribers and relying parties:

i. discontinuation of certification operations using the compromised private key;

ii. revocation of all certificates;

iii. investigation of the cause of compromise;

iv. formulation of proposed remedial measures and evaluation/approval thereof by CTJ PA;

v. execution of remedial measures;

vi. assessment on appropriateness of resuming business operations;

vii. accepting new application for this service, generation of new key pairs and providing the Subordinate CA;

viii. resumption of certification operations (including notification to subscribers and Relying Parties); and

ix. reissuance of Subscriber Certificates

When the Subordinate CA suffers from a disaster, the Subordinate CA shall perform recovery operations using backup hardware, software and data based on the business continuation plan prescribed in "Business Continuity upon Disasters" 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.

5.7.1.2 In the event of Compromise of Root CA

When Cybertrust learns that the private key of the Root CA has been compromised, Cybertrust shall execute the following, and simultaneously notify the fact of such compromise to the browser vendor that has registered the Root CA Certificate, and publish the same in the repositories:

i. discontinuation of certification operations using the compromised private key;

ii. revocation of all certificates of the Subordinate CA that were issued after the launch of the Root CA; and

iii. examination, determination and implementation of measures (including, but not limited to, dealing with the Subordinate CA, investigation of the cause of compromise, corrective action, and method of resuming services).

When the Root CA suffers from a disaster, the Root CA shall perform recovery operations of backup key information 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 in the repositories when the certification operations are resumed.

5.7.2 Recovery Procedures if Computing Resource, Software, and/or Data Are Corrupted

When hardware, software or data is destroyed, the Certification Authorities shall recover the system through maintenance and by using backup data and the like and shall continue performing the certification operations.

5.7.3 Recovery Procedures After Key Compromise

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 revocation procedures of the Subscriber Certificate based on the procedures prescribed in "4.9 Certificate Revocation and Suspension" of this CPS.

The Subordinate CA revokes a Subscriber Certificate based on "4.9 Certificate Revocation and Suspension" of this CPS.

5.7.4 Business Continuity Capabilities after a Disaster

The Root CA shall separately set forth a business continuation plan regarding the recovery measures for recovering from disasters, and business continuity. The business continuation plan defines the operating procedures of recovery and resumption of all or a part (revocation processing) of the operations of the Root CA by using data and the like stored 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.

With regard to the business continuation plan for the Subordinate CA, the plan for Root CA shall apply correspondingly.

5.8 CA or RA Termination

When the Root CA is to terminate the operations of the Root CA, the Root CA shall publish information to such effect in advance on Cybertrust's website.

The Subordinate CA shall deem that the operation of the Subordinate CA has been terminated when the Subordinate CA terminates the use of this service.

The information of subscribers held by the Subordinate CA shall be abolished or provided to the transferee of business operations.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The key pair used in the Root CA was acquired by Cybertrust after JCSI terminated the provision of its service using the root certificate in 2014 as described in "1.1 Overview" of this CPS. In acquiring the key pair, Cybertrust prepared a private key cryptographic module ("HSM") that satisfies the standards of FIPS 140-2 Level 3 for managing the key pair of the Root CA, and transferred the key pair to Cybertrust's HSM, via the secrecy distribution method, from the HSM of the same standards that were being used by JCSI to control the key pair.

The key pair of the Root CA shall be transferred in the presence of the auditor set forth in "8.2 Identity/Qualifications of Assessor" and "8.3 Assessor's Relationship to Assessed Entity" of this CPS or, when the auditor is not available, by presenting to the auditor the transfer records and the recording of the key confirmation procedures so as to ensure that the transfer of the key pair of the Root CA was performed according to predetermined procedures based on Key Generation Script.

The key pair of an OCSP server certificate and the Subordinate CA Certificate shall be generated by multiple Issuing Authority System Administrators based on Certification Authority Supervisor's instructions under the control of the Issuing Authority Manager.

In generating the key pair of the Subordinate CA, the HSM that satisfies the standards of FIPS 140-2 Level 4 shall be used. In generating the key pair of the OCSP server, the HSM that satisfies the standards of FIPS 140-2 Level 3 shall be used.

The key pair of the Subordinate CA shall be generated in the presence of the auditor set forth in "8.2 Identity/Qualifications of Assessor" and "8.3 Assessor's Relationship to Assessed Entity" 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 Subordinate CA was performed according to predetermined procedures based on Key Generation Script.

6.1.1.2 RA Key Pair Generation

Not Applicable.

6.1.1.3 Subscriber Key Pair Generation

The Subordinate CA will reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

This Subordinate CA rejects a certificate request if one or more of the following conditions on generation of subscriber's key pair are met;

i. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6 of the BRs;

ii. There is clear evidence that the specific method used to generate the Private Key was flawed;

iii. This Subordinate CA Authority is aware of a demonstrated or proven method that exposes the Applicant's Private to compromise;

iv. This Subordinate CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of "4.9.1.1 Reasons for Revoking a Subscriber Certificate" of this CP; or

v. This Subordinate CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

This Subordinate CA does not generate the key pair used in a Subscriber Certificate when the certificate profile containing an extKeyUsage extension which includes either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280]. This Subordinate CA does not also accept the certificate request when the subscriber's key pair is previously generated by this Subordinate CA.

6.1.2 Private Key Delivery to Subscriber

The Subordinate CA does not deliver a subscriber's private key. A subscriber's private key shall be generated independently by the subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

A subscriber shall include the public key in the data for requesting the issuance of a Certificate, and then deliver the same to the Subordinate CA via email.

6.1.4 Certification Authority Public Key Delivery to Relying Parties

The Subordinate CA does not deliver the public key of the Subordinate CA to Relying Parties.

The certificates of the Root CA including the public key of the Root CA is published in the repositories.

6.1.5 Algorithm Type and Key Sizes

6.1.5.1 Root CA Certificates

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

Certification Authority Name	Signature Algorithm	Key Length
SecureSign RootCA11	SHA1 with RSA	2048 bit (with a modulus size in bits divisible by 8)

6.1.5.2 Subordinate CA Certificates

The key signature algorithm and key length of the Subordinate CA Certificate shall be as follows.

Subordinate CA Certificate	Signature Algorithm	Key Length
The Subordinate CA Certificate issued by SecureSign RootCA11	SHA2 with RSA	2048 bit (with a modulus size in bits divisible by 8)

6.1.5.3 Subscriber Certificates

The key signature algorithm and key length of the Subscriber Certificate shall be as follows.

Subscriber Certificate	Signature Algorithm	Key Length
Subscriber Certificate issued by the Subordinate CA	SHA2 with RSA	2048 bit (with a modulus size in bits divisible by 8)

6.1.5.4 OCSP Server Certificates

The key signature algorithm and key length of an OCSP server certificate shall be as follows.

OCSP Server Certificate	Signature Algorithm	Key Length
OCSP server certificate issued by SecureSign RootCA11 or the Subordinate CA	SHA2 with RSA	2048 bit (with a modulus size in bits divisible by 8)

6.1.6 Public Key Parameters Generation and Quality Checking

The Certification Authorities shall confirm that the value of the public exponent is an odd number equal to 3 or more. And the public exponent shall be in the range between 2^16+1 and 2^256-1. The modulus shall also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

6.1.7 Key Usage Purposes

The key usage of the Root CA Certificate shall be Certificate Signing, CRL Signing.

The key usage of the Subordinate CA certificate shall be Certificate Signing, CRL Signing.

The key usage of Subscriber Certificate shall be Digital Signature, Key Encipherment.

The key usage of an OCSP server certificate shall be Digital Signature.

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 pair of the Root CA shall be the HSM that satisfies the FIPS 140-2 Level 3 standard. The HSM shall be controlled by the Issuing Authority.

The cryptographic module for controlling the key pair of the Subordinate CA shall be the HSM that satisfies the FIPS 140-2 Level 4 standard. The HSM shall be controlled by the Issuing Authority.

The key pair of an OCSP server certificate shall be controlled by the HSM that satisfies the FIPS 140-2 Level 3 standard. The OCSP server shall be controlled by the Issuing Authority.

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

The private key used by the Certification Authorities and the OCSP servers shall at all-time be controlled by multiple Issuing Authority System Administrators.

6.2.3 Private Key Escrow

The Certification Authorities do not deposit the private key used by the Certification Authorities and the OCSP servers or deposit 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 Authorities. The private key backed up from the HSM shall be encrypted and then divided into multiple pieces, and safely stored in a lockable safe.

The private key to be used in an OCSP server is backed up and archived by the Issuing Authority System Administrator in an encrypted state as the backup of the system.

6.2.5 Private Key Archival

The Certification Authorities shall not archive the private key used by the Certification Authorities and the OCSP servers.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The Root CA shall not generate the Private Key on behalf of the Subordinate CA.

The Certification Authority transfers a copy of the private key used by the Certification Authority to the backup site based on a safe method. When it is necessary to restore the private key of the Certification Authority due to a failure of the HSM or other reasons, the Issuing Authority System Administrator shall restore the private key using the backup stored in the main site or the backup site.

When the recovery of the private key of an OCSP server is required, the Issuing Authority System Administrator shall perform such recovery by using the system backup archived in the main site; provided, however, that, based on the approval of the Certification Authority Supervisor, there may be cases where the corresponding certificate is revoked, and a private key is newly generated.

6.2.7 Private Key Storage on Cryptographic Module

The private key of the Root CA and the OCSP servers shall be stored in the HSM that satisfies the standards of FIPS 140-2 Level 3.

The private key of the Subordinate CA shall be stored in the HSM that satisfies the standards of FIPS 140-2 Level 4.

6.2.8 Activating Private Keys

The private key used by the Certification Authorities and the OCSP servers 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 Deactivating Private Keys

The private key used by the Certification Authorities and the OCSP servers shall be deactivated by multiple Issuing Authority System Administrators based procedures to be separately prescribed based on the approval of the Issuing Authority Manager. The deactivation operation shall be recorded.

6.2.10 Destroying Private Keys

The private key used by the Certification Authority and the OCSP server 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 of the Certification Authority 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 Capabilities

The Certification Authorities 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 including that public key.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the key pair of the Root CA shall be as follows.

Key Pair	Validity Period

Key Pair of the Root CA	April 8, 2029

The validity period of the key pair of the Subordinate CA shall be as follows.

Key Pair	Validity Period
Key Pair of the Subordinate CA	No later than April 8, 2029

The validity period of the OCSP server certificate shall be as follows.

Certificate	Validity Period
OCSP Server Certificate	Within 25 months

The validity period of the Subscriber Certificate shall be as follows.

Certificate	Validity Period
Subscriber Certificate	Within 398 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used by the Certification Authorities shall be created 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 Authorities 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.

6.4.3 Other Aspects of Activation Data

Not Applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

i. authentication of authority of the operator;

ii. identification and authentication of the operator;

iii. acquisition of operation logs for important system operations;

iv. setup of appropriate passwords; and

v. backup and recovery.

6.5.2 Computer Security Rating

The Certification Authorities shall implement, in advance, installation assessment of hardware and software to be installed by the Certification Authorities. The Certification Authorities shall also continuously collect information and perform evaluations regarding the security vulnerability in the system to be used, and take necessary measures based on the evaluation results.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The construction and change of the 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 confirm that there are no security-related problems.

6.6.2 Security Management Controls

The 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, the Certification Authorities shall continuously collect information and perform evaluations regarding the security vulnerability, and take necessary measures based on the evaluation results.

6.6.3 Life Cycle Security Controls

The Certification Authorities shall appoint a supervisor in the respective processes of development, operation, change, and disposal of the 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 Root CA system shall not be connected to a network and shall be operated offline.

The Subordinate CA system, OCSP server system and external systems such as the internet shall be connected via a firewall or the like and be monitored by an intrusion detection system.

6.8 TimeStamping

According to "5.5.5 Requirements for Time-stamping of Records" of this CPS.

7. Certificate, CRL, and OSCP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Matters are described in Appendix B.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

The Certification Authority uses certificate extensions in accordance with applicable industry standards, including RFC 5280. The Certification Authority does not issue Certificates with a critical private extension.

Certificates must contain the ExtendedKeyUsage extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. Certificates may not contain the anyExtendedKeyUsage value. Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: must contain an EKU extension; must not include the anyExtendedKeyUsage; and, must not include both the id-kp-serverAuth and id-kp-emailProtection in KeyPurposeId in the same certificate at the same time.

Technically Constrained Subordinate CA Certificates shall include, in Extended Key Usage (EKU) extension, all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId shall not appear in the EKU extension of publicly trusted certificates.

For the Subscriber certificates, the subjectAltName extension is populated in accordance with RFC 5280. The SubjectAltName extension is populated with the authenticated value of the domain name in the Common Name field of the subject DN (either domain name or public iPAddress applicable). The SubjectAltName extension may contain additional authenticated domain names or public iPAddresses. For internationalized domain names, the value encoded by Punycode algorithm shall be listed in the SubjectAltName extension as a Punycode(A-label) value.

Matters regarding the certificates of the Certification Authority are described in Appendix B.

7.1.3 Algorithm Object Identifier

This Certification Authority signs Certificates using SHA256 with RSA in accordance with the Mozilla Root Store Policy and the Relevant Requirements.

Matters are described in Appendix B.

Note that the Root CA shall not issue any Subordinate CA certificates using the SHA-1 hash algorithm and Subordinate CA shall not issue any Subscriber Certificates using the SHA-1 hash algorithm.

7.1.4 Name Forms

This Certification Authority uses distinguished names that are composed of standard attribute types, such as those identified in RFC 5280. The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuer Certification Authority to support name chaining as specified in section 4.1.2.4 of RFC 5280. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1.

For the Subscriber certificates, the subjectAltName extension must be present and contain at least one FQDN, and the FQDN included in the certificate shall be validated based on section 3.2.2.4 of this CPS.

Matters are described in Appendix B.

Note that underscore characters ('_') must not be present in dNSName entries.

Subject attributes must not contain only metadata such as '.' (i.e. period), '-' (i.e. hyphen), and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

Other attributes may be present within the subject field. If present, other attributes must contain information that has been verified by the Certification Authorities.

7.1.5 Name Constraints

The Subordinate CA includes name constraint in the nameConstarints field in the Subordinate CA Certificate.

7.1.6 Certificate Policy Object Identifier

The policy object identifier of the Subscriber Certificate shall be as prescribed in "1.2 Document Name and Identification" of this CPS.
In addition, it includes {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} - 2.23.140.1.2.2 definded by CA/Browser Forum.

i. A Certificate to a Subordinate CA that is not an Affiliate of the Root CA:

- shall include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with BR and
- shall not contain the "anyPolicy" identifier (2.5.29.32.0).

ii. A Certificate to a Subordinate CA that is an affiliate of the Root CA:

- contains the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

iii. The policy object identifier of the Root CA Certificate shall be as prescribed in "1.2 Document Name and Identification" of this CPS.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Matters are described in Appendix B.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

Effective on 2020-09-30, for revoked Subscriber Certificates, the CRLReason indicated MUST NOT be unspecified (0) or certificateHold (6). If the reason for revocation is unspecified, the Certification Authority MUST omit reasonCode entry extension, if allowed by the previous requirements.

On-or -after 2020-09-30, the CRLReason must indicate one of following reason codes which is the most appropriate reason for revocation of the certificate listed in RFC5280, section 5.3.1 if a reasonCode CRL entry extension is present.

i. keyCompromise (1),

ii. cACompromised (2)

iii. affiliationChanged (3),

iv. superseded (4),

v. cessationOfOperation (5),

7.2.1 Version Number(s)

Matters are set forth in Appendix B.

7.2.2 CRL and CRL Entry Extensions

Matters are set forth in Appendix B.

7.3 OCSP Profile

Issuer CAs shall operate an OCSP service in accordance with RFC 6960.

Effective 2020-09-30, for publicly-trusted SSL/TLS Server Certificate, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus shall be present and asserted.

Effective 2020-09-30, for publicly-trusted SSL/TLS Server Certificate, the CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2 of this CPS.

7.3.1 Version Number(s)

Matters are set forth in Appendix B.

7.3.2 OCSP Extensions

Matters are set forth in Appendix B.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The Root CA verifies the Trust Service Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security once a year, or performing a visiting audit at the timing deemed necessary by the auditor "8.2 Identity/Qualifications of Assessor" of this CPS.

The Subordinate CA, which is the Technically Constrained Subordinate CA, conduct an audit set forth in the BR 8.7 in accordance with the BR 8.1.

8.2 Identity/Qualifications of Assessor

A Qualified Auditor shall verify the Trust Service Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities as described at BR 8.2.

8.3 Assessor’s Relationship to Assessed Entity

The auditor shall be, as a general rule, a party that is independent from the operations of the Certification Authorities and capable of maintaining neutrality.

8.4 Topics Covered by Assessment

The scope of audit for the Root CA shall be the scope set forth in the Trust Service Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

The scope of audit for the Subordinate CA shall be in accordance with the BR 8.7.

8.5 Actions Taken As A Result Of Deficiency

Identified matters that are discovered in the verification shall be reported to the CTJ PA, the Certification Authority Supervisor, the Issuing Authority Manager and the Registration Authority Manager. When the auditor, the 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 Communications of Results

Verification results of the Trust Service Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security shall be published according to the provisions of the respective guidelines.

8.7 SELF-AUDITS

During the period in which the Subordinate CA issues Subscriber Certificates, the Subordinate CA shall monitor adherence to its CPS and BR and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Subscriber Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. Other Business and Legal Matters

9.1 Fees

The fees for this service shall be notified so that a subscriber can properly verify the same.

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 Authorities. 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 Authorities shall handle the following information as confidential information (the "Confidential Information"):

i. application information;

ii. information set forth in "9.4.2 Information Treated as Private" of this CPS;

iii. inquiry information received from a third party (including Relying Parties); and

iv. information relating to the security of the Certification Authorities.

9.3.2 Information not within the Scope of Confidential Information

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

i. information set forth as in "2.2 Publication of Information" of this CPS as information to be published;

ii. the Subscriber Certificate, The Subordinate CA Certificate and the Root CA Certificate;

iii. information which became public knowledge due to reasons other than the negligence on the part of the Certification Authorities;

iv. information which became public knowledge without any restriction of confidentiality from a party other than the Certification Authorities; and

v. information for which the subscriber and/or Relying Party 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 Authorities shall take measures for preventing the divulgence of the Confidential Information. The Certification Authorities 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/acquire 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 party 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 set forth in "9.4 Privacy 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 Authorities shall be set forth in the Privacy Policy that is published on Cybertrust's website (https://www.cybertrust.co.jp/corporate/privacy-policy.html).

9.4.2 Information Treated as Private

The Certification Authorities shall handle, as personal information, any information that is included in inquiries or the like capable of identifying a specific individual.

Note that the Certification Authorities shall treat a data, including IP addresses, from OCSP requests by the Relying Parties as personal data, in accordance with the General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/679. Cybertrust Japan does not use these data in server logs to build profiles or identify individuals. The server logs are used for operational purposes only and are normally kept at least until next audit. After that, the server logs are deleted in accordance with Cybertrust's internal rules.

9.4.3 Information not Deemed Private

The Certification Authorities 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 Authorities 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 Authorities has obtained the consent of the subscriber with regard to the Certification Authorities using the personal information of that subscriber for performing its certificate issuance/revocation operations that are scheduled in this CPS and the Certification Authorities conducting an audit.

Moreover, the Certification Authorities shall not use the acquired personal information for any purpose other than for performing the certification operations; save for the case 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 Authorities 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 Authorities are to outsource a part of its operations, there may be cases where the Certification Authorities need to disclose the Confidential Information to the outsourcee. In the foregoing case, the Certification Authorities 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 related to this service shall belong to Cybertrust related to this service:

i. this CPS;

ii. public key and private key of the Certification Authorities; and

iii. certificates issued by the Certification Authorities and revocation information on and after the launch date.

9.6 Representations and Warranties

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

9.6.1 Issuing Authority Representations and Warranties

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

i. to safely control the Certification Authorities private key;

ii. to perform accurate certificate issuance and revocation based on the application from the Registration Authority;

iii. to provide revocation information by the CRL and the OCSP server;

iv. to monitor and operate the Certification Authorities system; and

v. to maintain and control the repositories.

9.6.2 Registration Authority Representations and Warranties

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

i. perform screening of subscribers based on this CPS;

ii. properly handle certificate issuance applications and revocation requests to the Issuing Authority; and

iii. accept inquiries ("1.5.2 Contact Persons" of this CPS).

9.6.3 Subscriber Representations and Warranties

Subscriber represents and warrants that it bears the following obligations:

i. provide true and accurate information upon applying for the issuance of a Subscriber Certificate;

ii. strictly manage the private key and password to ensure the confidentiality and safety thereof;

iii. refrain from installing a Subscriber Certificate in a server and using the Subscriber Certificate until the accuracy of the information included in the certificate is confirmed;

iv. install a Subscriber Certificate only in a server that is accessible by the subjectAltName included in the Subscriber Certificate, and use the Subscriber Certificate in according with the applicable law and regulations and the Subscriber Agreement;

v. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;

vi. promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise;

vii. respond to the Certification Authority's instruction within a specified period upon the occurrence of an event set forth in "4.9.1.1 Reasons for Revoking a Subscriber Certificate" of this CP;

viii. acknowledge and accept that the Certification Authority is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the Certification Authority's CPS, or relevant requirements set forth by CA/Browser Forum;

ix. refrain from including the organization unit (OU) in Subscriber Certificate;

x. comply with the usage of the Subscriber Certificate ("1.4.2 Appropriate Certificate Uses" of this CPS);

xi. refrain from using the Subscriber Certificate in websites and emails that are offensive to public order and morals;

xii. refrain from using an expired Subscriber Certificate or a revoked Subscriber Certificate; and

xiii. observe applicable laws and regulations.

9.6.4 Relying Party Representations and Warranties

The Relying Parties represent and warrant that they bear the following obligations:

i. to confirm whether the certificate is used for the for the usage set forth in "1.4.2 Appropriate Certificate Uses" of this CPS;

ii. to confirm the effective period and entries of the Subordinate CA;

iii. to verify the digital signature and confirm the issuer of the Certification Authority certificate;

iv. to confirm whether the certificate has been revoked based on CRL or the OCSP server; and

v. to bear legal liability for situations arising from the default of obligations prescribed in this paragraph.

9.6.5 Representations and Warranties of Other Relevant Parties

Not applicable.

9.7 Disclaimers of Warranties

The Certification Authorities 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 "9.6.1 Issuing Authority Representations and Warranties" and "9.6.2 Registration Authority Representations and Warranties" of this CPS.

The Certification Authorities shall not be liable in any way for the consequences resulting from a relying party trusting the Certification Authority certificate 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 "9.6.1 Representations and Warranties of Issuing Authority" and "9.6.2 Registration Authority Representations and Warranties" of this CPS:

i. any damage that arises regardless of the Certification Authorities observing this CPS and legal regulations;

ii. any damage that arises due to fraud, unauthorized use or negligence that is not attributable to Cybertrust;

iii. damage that arises as a result of the Relying Parties neglecting to perform their respective obligations prescribed in "9.6 Representations and Warranties" of this CPS;

iv. damage that arises as a result of the key pair of the certificate issued by the Certification Authorities being divulged or compromised due to acts of a third party other than Cybertrust;

v. damage that arises as a result of the certificate infringing upon the copyright, trade secret or any other intellectual property right of subscribers, a Relying Party or a third party; or

vi. damage caused by the weakening of the cryptographic strength resulting from technological advances such as improvement in the encryption algorithm decoding technology, or by any other vulnerability of the encryption 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 this service and/or the certificates shall not exceed 10,000,000 yen under no circumstances whatsoever.

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 Certification Authorities 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 Relying Party receives or uses the Certification Authority certificate, that 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:

i. unauthorized use, falsification, or misrepresentation during the use of the Certification Authority certificate;

ii. breach of this CPS. breach of this CPS or the Subscriber Agreement; or

iii. neglect by a subscriber to preserve the private key.

The Certification Authority is not the 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 the 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 Root CA 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 Notices and Communications with Participants

When Cybertrust is to notify subscribers individually, such notice shall deem 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 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 Procedure for Amendment

The Root CA shall amend this CPS on instructions from the CTJ PA at least once a year to meet the various requirements, also increment its version number and add a dated changelog entry. The 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 as needed.

9.12.2 Notification Mechanism and Period

After the CTJ PA approves the amendment of this CPS, the Root CA shall take measures to post the CPS before amendment and the CPS after amendment for a given period on the website so that the Relying Parties can confirm the amended contents. The amended CPS shall come into force at the time that is set forth by the CTJ PA unless the withdrawal of the amended CPS is publicly announced by Cybertrust.

9.12.3 Circumstances Under which Object Identifier Must Be Changed

CTJ PA is responsible to decide if the OID updates are required correspondingly to this CPS change.

9.13 Dispute Resolution Procedures

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

This CPS is subject to all applicable laws and regulations.

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)

Cybertrust may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Cybertrust's failure to enforce a provision of this CPS does not waive Cybertrust's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by Cybertrust.

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, labour disputes, or other reasons that are not attributable to Cybertrust, 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 third party that trusted or used the certificate.

9.17 Other Provisions

Not Applicable.

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 effective period 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 effective period 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 confirm 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 applications, screening 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.
Policy Authority (CTJ PA)	The committee set forth by Cybertrust that supervise the Certification Authority and reviews/approves the policy with independent from the Certification Authority.
Main Site	A facility equipped with assets of the Certification Authorities required for certificate issuance and revocation.

Escrow	As used herein, the term "escrow" 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.
ACME	Abbreviation for "Automated Certificate Management Environment" and it is a standard protocol for automate the processes of domain names verification, installation, and management for X.509 certificates.
ALPN	Abbreviation for "Application-Layer Protocol Negotiation" and it is an extended function of TLS.
Baseline Requirements	“Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”. Requirements for issuing publicly-trusted certificates which are formulated by the CA/Browser Forum and the latest version shall be adopted in this CPS.
CAA contactemail Property	The CAA contactemail property takes an email address as its parameter. The entire parameter value must be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used. SYNTAX: contactemail <rfc6532emailaddress> The following is an example where the holder of the domain specified the contact property using an email address. $ORIGIN example.com. CAA 0 contactemail "domainowner@example.com" The contactemail property may be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.
CA/Browser Forum	A voluntary group of certification authorities, vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing. It conducts activities such as adaptation of EV Guidelines and Baseline Requirements. The URL is https://www.cabforum.org .
Certification Authority Authorization Resource Record (CAA Record)	One of the DNS records defined in RFC8659 which aims to clarify the certification authority to issue the server certificate to a domain name and prevent the issuance of unintended certificates.
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.
DNS TXT Record Email Contact	The DNS TXT record must be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record must be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.
DNS TXT Record Phone Contact	The DNS TXT record must be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record must be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used.
FIPS 140-2	FIPS 140 (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 140-2. 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.

IP Address Contact	The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.
IP Address Registration Authority	The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
ITU-T	Telecommunications Standardization Sector of the International Telecommunication Union.
JCSI SSL/TLS Certificate	The SSL/TLS Certificate issued from JCSI Subordinate CA.
The JCSI Certificate Issuing Service	The Cybertrust's service which provides JCSI Subordinate CA, which is Technically Constrained Subordinate CA, for a Subscriber to get and use a JCSI SSL/TLS Certificates. Cybertrust provides the JCSI Certificate Issuing Service to a Subscriber who gets and use the JCSI SSL/TLS Certificates, however Cybertrust shall not provide this service to any organization other than the Subscriber who has the domain which is registered and restricted as "Technically Constrained".
JCSI Subordinate CA	The Subordinate CA which is the Technically Constrained Subordinate CA and issued under the JCSI Root CA.
OCSP	Abbreviation of "Online Certificate Status Protocol", and is a communication protocol for providing certificate revocation information.
RFC7231	The document named "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content" defining semantics of HTTP/1.1 message which is set forth by the IETF PKIX Working Group.
RFC7538	The document named "The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)" defining the additional Hypertext Transfer Protocol (HTTP) status code 308 (Permanent Redirect) which is set forth by the IETF PKIX Working Group.
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.
SSL/TLS	A protocol for encrypting and sending/receiving information online which was developed by Netscape Communications. TLS is an improvement of SSL 3.0.
Technically Constrained Subordinate CA	The Technically Constrained Subordinate CA Certificate set forth in the Baseline Requirements. That is, the Subordinate CA which uses the Subordinate CA Certificate containing Key Usage Extension and Name Constraint Extension in it to constrain the issuance of Subscriber Certificates.
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.

WEBTRUST FOR CERTIFICATION AUTHORITIES – SSL BASELINE REQUIREMENTS AUDIT CRITERIA	Requirements for issuing and managing publicly-trusted certificates which were formulated by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.
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.

Appendix B: Profile of Certificates

SecureSign RootCA11

Root CA Certificate (Effective Period: April 8, 2009 to April 8, 2029)

(Standard Area)

Version		**value**
Version	version of the encoded certificate type:INTEGER value:2	 2 (Ver.3)
Serialnumber		**value**
CertificateSerialNumber	serial number of certificate type:INTEGER value: unique positive integer	 1 (0x01)
Signature		**value**
AlgorithmIdentifier	the identifier for the crypto-graphic algorithm used by the CA to sign this certificate	
Algorithm	Object ID for the cryptographic algorithm (SHA-1) type:OID value:1 2 840 113549 1 1 5	 1.2.840.113549.1.1.5
parameters	Parameters of cryptographic algorithm type:NULL value:	 NULL
Issuer		**value**
CountryName	Country-name attribute of certificate issuer	
type	Object ID for the country name type:OID value:2 5 4 6	 2.5.4.6
value	Value of country name type:PrintableString value:JP	 JP
OrganizationName	Organization-name attribute of certificate issuer	
type	Object ID for the organization name type:OID value:2 5 4 10	 2.5.4.10
value	Value of organization name type:PrintableString value: Japan Certification Services, Inc.	 Japan Certification Services, Inc.
CommonName	Common-name attribute of certificate issuer	
Type	Object ID for the common name type:OID value:2 5 4 3	 2.5.4.3
value	Value of common name type:PrintableString value: SecureSign RootCA11	 SecureSign RootCA11
Validity		**value**
Validity	Validity period of certificate	
notBefore	the date on which the certificate validity period begins type:UTCTime value:090408045647Z	 April 8th 2009, 04:56:47(GMT)
notAfter	the date on which the certificate validity period ends type:UTCTime value:290408045647Z	 April 8th 2029, 04:56:47(GMT)
Subject		**value**
CountryName	Country-name attribute of certificate subject	
type	Object ID for the country name type:OID value:2 5 4 6	 2.5.4.6
value	Value of country name type:PrintableString value:JP	 JP
OrganizationName	Organization-name attribute of certificate subject	
type	Object ID for the organization name type:OID	

	value:2 5 4 10	2.5.4.10
value	Value of organization name type:PrintableString	
	value: Japan Certification Services, Inc.	Japan Certification Services, Inc.
CommonName	Common-name attribute of certificate subject	
type	Object ID for the common name type:OID	
	value:2 5 4 3	2.5.4.3
value	Value of common name type:PrintableString	
	value: SecureSign RootCA11	SecureSign RootCA11
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject's public key information	
AlgorithmIdentifier	the identifier for the cryptographic algorithm	
algorithm	Object ID for the 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	Value of public key type: BIT STRING	
	value: public key	2048Bit length of public key

(Expansion Area)

subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**value**
SubjectKeyIdentifier	Subject Key Identifier	
keyIdentifier	the identifier for the public key type:OctetString	
	value: hash of the value of the BIT STRING subjectPublicKey	5b f8 4d 4f b2 a5 86 d4 3a d2 f1 63 9a a0 be 09 f6 57 b7 de
keyUsage (extnId :== 2 5 29 15, critical :== TRUE)		**value**
KeyUsage	the purpose of the key contained in the certificate. type:BitString	
	value:000001100 (keyCertSign,cRLSign)	000001100
basicConstraints (extnId :== 2 5 29 19, critical :== TRUE)		**value**
BasicConstraints	Basic Constraints	
cA	The flag to determine whether the supplied certificate is associated with a CA or an end entity type:Boolean	
	value: True (associated with the CA)	TRUE

CRL

(Standard Area)

Version		**value**
Version	version of the encoded certificate/CRL type:INTEGER value:1	 1 (Ver.2)
Signature		**value**
AlgorithmIdentifier	the identifier for the crypto-graphic algorithm used by the CA to sign this certificate	
Algorithm	Object ID for the cryptographic algorithm (SHA-1) type:OID value:1 2 840 113549 1 1 5	 1.2.840.113549.1.1.5
parameters	Parameters of cryptographic algorithm type:NULL value:	 NULL
Issuer		**value**
CountryName	Country-name attribute of certificate issuer	
type	Object ID for the country name type:OID value:2 5 4 6	 2.5.4.6
value	Value of country name type:PrintableString value:JP	 JP
OrganizationName	Organization-name attribute of certificate issuer	
type	Object ID for the organization name type:OID value:2 5 4 10	 2.5.4.10
value	Value of organization name type:PrintableString value: Japan Certification Services, Inc.	 Japan Certification Services, Inc.
CommonName	Common-name attribute of certificate issuer	
type	Object ID for the common name type:OID value:2 5 4 3	 2.5.4.3
value	Value of common name type:PrintableString value: SecureSign RootCA11	 SecureSign RootCA11
ThisUpdate		**value**
ThisUpdate	the issue date of this CRL type:UTCTime value:yymmddhhmmssZ	
NextUpdate		**value**
NextUpdate	the date by which the next CRL will be issued type:UTCTime value:yymmddhhmmssZ	 (12 month)

(Expansion Area)

authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier	Certification Authority Key Identifier	
keyIdentifier	the identifier for the public key of CA which issued CRL type:OctetString value: hash of the value of the BIT STRING CA-PublicKey	 5b f8 4d 4f b2 a5 86 d4 3a d2 f1 63 9a a0 be 09 f6 57 b7 de
cRLNumber (extnId :== 2 5 29 20, critical :== FALSE)		**value**
cRLNumber	serial number of CRL type:INTEGER value: unique positive integer	

(Entry Area)

RevokedCertificates		**value**
CertificateSerialNumber	serial number of revoked certificate type:INTEGER value: unique positive integer	
revocationDate	The date on which the revocation occurred type:UTCTime value:yymmddhhmmssZ	

(Entry Expansion Area)

invalidityDate (extnId :== 2 5 29 24, critical :== FALSE)		**value**
invalidityDate	the date on which it is known or suspected that the certificate became invalid type:GeneralizedTime value:yyyymmddhhmmssZ	
cRLReason (extnId :== 2 5 29 21, critical :== FALSE)		**value**
cRLReason	the reason for the certificate revocation type: Enumerated value: reason code for the revocation	

OCSP Server Certificate

(Standard Area)

Version		**value**
Version	Version of the encoded certificate type:INTEGER value:2	 2 (Ver.3)
Serialnumber		**value**
CertificateSerialNumber	Serial number of certificate type:INTEGER value: unique positive integer	 *serial number 41 (0x29)
Signature		**value**
AlgorithmIdentifier algorithm parameters	The identifier for the crypto-graphic algorithm used by the CA to sign this certificate (public key cryptosystem and hash) Object ID for the cryptographic algorithm (SHA-2) type:OID type:1 2 840 113549 1 1 11 Parameters of cryptographic algorithm type:NULL value:	 sha256WithRSAEncryption NULL
Issuer		**value**
CountryName type value OrganizationName type value CommonName type value	Country-name attribute of the certificate issuer Object ID for the country name type:OID value:2 5 4 6 Value of country name type:PrintableString value:JP Organization-name attribute of the certificate issuer Object ID for the country name type:OID value:2 5 4 10 Value of organization name type:PrintableString value: Japan Certification Services, Inc. Common-name attribute of the certificate issuer Object ID for the common name type:OID value:2 5 4 3 Value of common name type:PrintableString value: SecureSign RootCA11	 2.5.4.6 JP 2.5.4.10 Japan Certification Services, Inc. 2.5.4.3 SecureSign RootCA11
Validity		**value**
Validity notBefore notAfter value:190331145959Z	Validity period of certificate the date on which the certificate validity period begins type:UTCTime value:160306064915Z The date on which the certificate validity period ends type:UTCTime	 *the date on which the certificate validity period begins March 6, 2017, 06:49:15(GMT) *the date on which the certificate validity period ends March 31, 2019, 14:59:59(GMT)
Subject		**value**
CountryName type value OrganizationName type value	Country-name attribute of the certificate issuer Object ID for the country name type:OID value:2 5 4 6 Value of country name type:PrintableString value:JP Organization-name attribute of certificate issuer Object ID for the organization name type:OID value:2 5 4 10 Value of organization name	 2.5.4.6 JP 2.5.4.10

	type:PrintableString value: Japan Certification Services, Inc.	Japan Certification Services, Inc.
CommonName	Common-name attribute of the certificate issuer	
type	Object ID for the common name type:OID value:2 5 4 3	2.5.4.3
value	Value of common name type:PrintableString value:SecureSign RootCA11 OCSP Responder	SecureSign RootCA11 OCSP Responder
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject's public key information	
AlgorithmIdentifier	The identifier for the cryptographic algorithm(public key cryptosystem and hash)	
algorithm	Object ID for the 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	Value of public key type: BIT STRING value: public key	public key of 2048 bit length

(Expansion Area)

basicConstraints (extnId :== 2 5 29 19, critical :== FALSE)		**value**
BasicConstraints cA	Basic Constraints The flag to determine whether the supplied certificate is associated with a CA type:Boolean value: FALSE(not associated with the CA)	FALSE
authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
authorityKeyIdentifier keyIdentifier	Certification Authority Key Identifier The identifier for the public key type:OctetString value: Hash of the value of certificate issuer's PublicKey	5b f8 4d 4f b2 a5 86 d4 3a d2 f1 63 9a a0 be 09 f6 57 b7 de
subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**value**
SubjectKeyIdentifier keyIdentifier	Subject Key Identifier The identifier for the public key type:OctetString value: Hash of the value of the subject's PublicKey	B9:49:42:CC:DD:D7:42:9F:7D:A1: 8F:E3:B6:08:F5:C9:BA:26:55:96
keyUsage (extnId :== 2 5 29 15, critical :== FALSE)		**value**
KeyUsage	The purpose of the key type:BitString value:100000000 (digitalSignature)	100000000
extKeyUsage (extnId :== 2 5 29 31, critical :== FALSE)		**value**
extendedKeyUsage	Purpose of the key usage (extension)	
KeyPurposeID OCSPSigning	ID for the purpose of the key usage type:OID value: Online responder signature usage	1.3.6.1.5.5.7.3.9
OCSP No Check (extnId :== 1.3.6.1.5.5.7.48.1.5 , critical :== FALSE)		**value**
OCSP No Check OCSP No Check	Revocation checking of signer's certificates Do not check revocation	NULL

JCSI Subordinate CA Certificate (reference)

(Standard Area)

Version		**value**
Version	version of the encoded certificate type:INTEGER value:2	 2 (Ver.3)
SerialNumber		**value**
CertificateSerialNumber	serial number of certificate type:INTEGER value: unique positive integer	 *serial number(random serial number)
Signature		**value**
AlgorithmIdentifier Algorithm parameters	the identifier for the crypto-graphic algorithm used by the CA to sign this certificate (public key cryptosystem and hash) Object ID for the 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 OrganizationName type value CommonName Type value	Country-name attribute of certificate issuer Object ID for the country name type:OID value:2 5 4 6 Value of country name type:PrintableString value:JP Organization-name attribute of certificate issuer Object ID for the organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Japan Certification Services, Inc. Common-name attribute of certificate issuer Object ID for the common name type:OID value:2 5 4 3 Value of common name type:PrintableString Value: SecureSign RootCA11	 2.5.4.6 JP 2.5.4.10 Japan Certification Services, Inc. 2.5.4.3 SecureSign RootCA11
Validity		**value**
Validity notBefore notAfter 	Validity period of certificate the date on which the certificate validity period begins type:UTCTime value:yymmddhhmmssZ the date on which the certificate validity period ends type:UTCTime Value:yymmddhhmmssZ	 *the certificate validity period begins yymmddhhmmssZ (issuance date, time) *the certificate validity period ends 290408045647Z (April 8, 2029 4:56:47 GMT)
Subject		**value**
CountryName type value OrganizationName type value	Country-name attribute of certificate subject Object ID for the country name type:OID value:2 5 4 6 Value of country name type:PrintableString value:JP Organization-name attribute of certificate subject Object ID for the organization name type:OID value:2 5 4 10 Value of organization name	 2.5.4.6 JP 2.5.4.10

	type:PrintableString value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co.,Ltd.
CommonName	Common-name attribute of certificate subject	
type	Object ID for the common name type:OID value:2 5 4 3	2.5.4.3
value	Value of common name type:PrintableString value:JCSI TLSSign Public CA	JCSI TLSSign Public CA (exsample)
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject's public key information	
AlgorithmIdentifier	the identifier for the cryptographic algorithm(public key cryptosystem and hash)	
algorithm	Object ID for the 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	Value of public key type: BIT STRING value: public key	public key of 2048 bit length

(Expansion Area)

certificatePolicies (extnId :== 2 5 29 32, critical :== FALSE)		**value**
PolicyInformation	Information of the Policy	
policyIdentifier	type:OID value:2.5.29.32.0 (anyPolicy)	2.5.29.32.0
policyQualifiers	Information of the policy qualifiers	
policyQualifierID	Classification of policy qualifiers type:OID value: Object ID of CPS URI (id-qt-cps)	1.3.6.1.5.5.7.2.1
Qualifier	URI of CPS is published type:OctetString value:https://www.cybertrust.ne.jp/jcsi/repository.html	https://www.cybertrust.ne.jp/jcsi/repository.html
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1, critical :== FALSE)		**value**
Authority Information Access	Authority Information Access	
Ocsp	Online Certificate Status Protocol type:OID value:1.3.6.1.5.5.7.48.1 type:OctetString value: http://rtocsp.managedpki.ne.jp/OcspServer	1.3.6.1.5.5.7.48.1 http://rtocsp.managedpki.ne.jp/OcspServer
Caissuers	Access method type:OID value:1.3.6.1.5.5.7.48.2 type:OctetString value: http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt	1.3.6.1.5.5.7.48.2 http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt
extendedKeyUsage (extnId :== 2 5 29 37, critical :== FALSE)		**value**
extendedKeyUsage	key usage (extension)	
KeyPurposeID	Key Purpose ID Tyepe:OID	
serverAuth	Value: serverAuth	1.3.6.1.5.5.7.3.1
authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier	Certificate Authority Key Identifier	
keyIdentifier	the identifier for the public key of CA which issued CRL type:OctetString value: hash of the value of the BIT STRING CA-PublicKey	5b:f8:4d:4f:b2:a5:86:d4:3a:d2:f1:63:9a:a0:be:09:f6:57:b7:de
cRLDistributionPoints (extnId :== 2 5 29 31, critical :== FALSE)		**value**
cRLDistributionPoints	CRL Distribution Point	
DistributionPoint	CRL Distribution Point	
uniformResourceIdentifie	URI	

	type:OctetString value: http://rtcrl.managedpki.ne.jp/SecureSign AD/SecureSignRootCA11/cdp.crl	http://rtcrl.managedpki.ne.jp/SecureSign AD/SecureSignRootCA11/cdp.crl
subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**value**
SubjectKeyIdentifier keyIdentifier	Subject Key Identifier the identifier for the public key type:OctetString value: hash of the value of the BIT STRING subjectPublicKey	(hash value of subjectPublicKey)
basicConstraints (extnId :== 2 5 29 19, critical :== TRUE)		**value**
BasicConstraints cA PathLenConstraint	Basic Constraints The flag to determine whether the supplied certificate is associated with a CA or an end entity type:Boolean value: True (associated with the CA) PathLenConstraint type:INTEGER value:0 (do not have subordinate CA)	 TRUE 0
Name Constraints (extnId :== 2.5.29.30, critical :== TRUE)		**value**
Name Constraints Permitted Names Excluded Names	Name Constraints dNS Name Directory Name IP address (IPv4) IP address (IPv6)	 .managedpki.ne.jp O=Cybertrust Japan Co.,Ltd., L=Minato-ku, ST=Tokyo, C=JP 0.0.0.0/0.0.0.0 0:0:0:0:0:0:0:0/0
keyUsage (extnId :== 2 5 29 15, critical :== TRUE)		**value**
KeyUsage	the purpose of the key contained in the certificate type:BitString value:10000110 (Digital Signature,keyCertSign,cRLSign)	 10000110 (0x86)

JCSI SSL/TLS Certificate (reference)

(Standard Area)

Version		**value**
Version	version of the encoded certificate type:INTEGER value:2	 2 (Ver.3)
Serialnumber		**value**
CertificateSerialNumber	serial number of certificate type:INTEGER value: unique positive integer	 *serial number(random serial number)
Signature		**value**
AlgorithmIdentifier algorithm Parameters	the identifier for the crypto-graphic algorithm used by the CA to sign this certificate (public key cryptosystem and hash) Object ID for the 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 OrganizationName Type Value CommonName Type Value	Country-name attribute of certificate issuer Object ID for the country name type:OID value:2.5.4.6 Value of country name type:PrintableString value:JP Organization-name attribute of certificate issuer Object ID for the organization name type:OID value:2.5.4.10 Value of organization name type:PrintableString value: Cybertrust Japan Co., Ltd. Common-name attribute of certificate issuer Object ID for the common name type:OID value:2.5.4.3 Value of common name type:PrintableString value:JCSI TLSSign Public CA	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co.,Ltd. 2.5.4.3 JCSI TLSSign Public CA
Validity		**value**
Validity notBefore notAfter 	Validity period of certificate the date on which the certificate validity period begins type:UTCTime value:yymmddhhmmssZ the date on which the certificate validity period ends type:UTCTime value:yymmddhhmmssZ	* the validity period: 25 months, editable * the date and time on which the certificate validity period begins * the date and time on which the certificate validity period ends
Subject		**value**
CountryName Type value StateOrProvinceName type	Country-name attribute of certificate subject Object ID for the country name type:OID value:2.5.4.6 Value of country name type:PrintableString value: country name attribute of certificate subject State or Province –name attribute of certificate subject Object ID for the state or province name type:OID	 2.5.4.6 JP

	value:2.5.4.8	2.5.4.8
value	value of state or province name type:PrintableString / UTF8String value: state or province name attribute of certificate subject	Tokyo
LocalityName	Locality-name attribute of certificate subject	
type	Object ID for the locality name type:OID value:2.5.4.7	2.5.4.7
value	Value of locality name type:PrintableString / UTF8String value: locality name attribute of certificate subject	Minato-ku
OrganizationName	Organization-name attribute of certificate issuer	
type	Object ID for the organization name type:OID value:2.5.4.10	2.5.4.10
value	Value of organization name type:PrintableString / UTF8String value: organization name attribute of certificate issuer	Cybertrust Japan Co.,Ltd.
CommonName	Common-name attribute of certificate issuer	
type	Object ID for the common name type:OID value:2 5 4 3	2 5 4 3
value	Value of common name type:PrintableString value: common name attribute of certificate issuer	* FQDN of the SSL/TLS server * Note: domain: .managedpki.ne.jp
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject's public key information	
AlgorithmIdentifier	the identifier for the cryptographic algorithm(public key cryptosystem and hash)	
algorithm	Object ID for the 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	Value of public key type: BIT STRING value: Value of public key	* the key length is depended on application * the key length must be at least 2048-bit

(Expansion Area)

basicConstraints (extnId :== 2 5 29 19, critical :==TRUE)		**value**
BasicConstraints	Basic Constraints	
cA	The flag to determine whether the supplied certificate is associated with a CA or an end entity type:Boolean value: FALSE(not associated with the CA)	FALSE
certificatePolicies (extnId :== 2 5 29 32, critical :== FALSE)		**value**
PolicyInformation	Information of the Policy	
policyIdentifier	type:OID value:1.2.392.00200081.1.10.10	1.2.392.00200081.1.10.10
policyQualifiers	Information of the policy qualifiers	
policyQualifierID	Classification of policy qualifiers type:OID value: Object ID of CPS URI (id-qt-cps)	1.3.6.1.5.5.7.2.1
Qualifier	URI of CPS is published type: URL value: https://www.cybertrust.ne.jp/jcsi/repository.html	https://www.cybertrust.ne.jp/jcsi/repository.html
policyIdentifier	type:OID	

	value:2.23.140.1.2.2	2.23.140.1.2.2
subjectAltName (extnId :== 2.5.29.17, critical :== FALSE)		**value**
dnsName	dnsName type:IA5String value: common name attribute of certificate issuer	 * FQDN of the SSL/TLS server * Note: Domain: .managedpki.ne.jp
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1, critical :== FALSE)		**value**
Authority Information Access Ocsp	Authority Information Access Online Certificate Status Protocol type:OID value:1.3.6.1.5.5.7.48.1 type:OctetString value: http://jcsitlssignpublicca-ocsp.managedpki.ne.jp/OcspServer	 1.3.6.1.5.5.7.48.1 http://jcsitlssignpublicca-ocsp.managedpki.ne.jp/OcspServer
Caissuers	Access Method type:OID value:1.3.6.1.5.5.7.48.2 type:OctetString value: http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/SSAD-JCSITLS.crt	 1.3.6.1.5.5.7.48.2 http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/SSAD-JCSITLS.crt
keyUsage (extnId :== 2 5 29 15, critical :== TRUE)		**value**
KeyUsage	the purpose of the key contained in the certificate type:BitString value:1010000 (digitalSignature,keyEncipherment)	 1010000(0xa0)
extendedKeyUsage (extnId :== 2.5.29.37, critical :== FALSE)		**value**
extendedKeyUsage KeyPurposeID serverAuth clientAuth	in addition to or in place of the basic purposes indicated in the key usage extension field Key Purpose ID type:OID value:1.3.6.1.5.5.7.3.1 type:OID value:1.3.6.1.5.5.7.3.2	 1.3.6.1.5.5.7.3.1(serverAuth) 1.3.6.1.5.5.7.3.2(clientAuth)
authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier keyIdentifier	Certificate Authority Key Identifier the identifier for the public key type:OctetString value: hash of the value of the BIT STRING subjectPublicKey	 * hash value of the PublicKey of SubCA
cRLDistributionPoints (extnId :== 2 5 29 31, critical :== FALSE)		**value**
cRLDistributionPoints DistributionPoint uniformResourceIdentifie	CRL Distribution Point CRL Distribution Point URI type:OctetString value: http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/cdp.crl	 http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/cdp.crl
subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**value**
SubjectKeyIdentifier keyIdentifier	Subject Key Identifier the identifier for the public key type:OctetString value: hash of the value of the BIT STRING subjectPublicKey	 * hash value of subjectPublicKey