# JCSI Root CA

# Certification Practice Statement

Version 1.5

English Version

## Cybertrust Japan Co., Ltd.

June 1, 2018

# *Note

This “JCSI Root CA Certification Practice Statement Version 1.5” 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.

# 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" |

# Table of Contents

# 1. Introduction

## 1.1 Overview

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

The Certification Authority is a Public Root CA that is identified with the following Certification Authority name, serial number, effective period and other information, and Cybertrust will start operating the Certification Authority 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<br>BDF85BB1C365C7D811B3 |
| Hash value (SHA-256) | BF0FEEFB9E3A581AD5F9<br>E9DB7589985743D26108<br>5C4D314F6F5D7259AA42<br>1612 |

Note that the key pair and root certificate of the Certification Authority 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 root 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 root certificate and revocation information, and related materials, contracts, and correspondences), JCSI is liable for such services and contents, and the Cybertrust has no knowledge of the same and is not liable therefor. The Certification Authority 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 Certification Authority will issue certificates of a Subordinate CA (the "Subordinate CA"; and the entity operating the Subordinate CA is hereinafter referred to as the "Subordinate CA Operator") that issues certificates to subscribers. Unless separately provided for herein, the term "certificate" used herein shall mean the Subordinate CA certificate.

Furthermore, the Certification Authority will issue an OCSP server certificate that appends the digital signature to OCSP responses when the Certification Authority provides revocation information with regards to the Subordinate CA based on OCSP.

Under this JCSI Root CA Certification Practice Statement (this "CPS") Version 1.5, the Certification Authority shall not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA. Thus, the Certification Authority shall issue/revoke certificates upon amending this CPS.

The Certification Authority is based on the following statement and laws and ordinances:

(i) Current version of the guideline “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates” (the “Baseline Requirements”) currently formulated by the CA/Browser Forum (the “CAB Forum”).

(ii) this CPS; and

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

The Certification Authority complies with the latest version of the Baseline Requirements that is published on http://www.cabforum.org. When there is a discrepancy between this CPS and the Baseline Requirements, the Baseline Requirements have precedence of this CPS.

This CPS prescribes the operation of the Certification Authority on and after the launch date as well as the various requirements pertaining thereto. The requirements include obligations of the Certification Authority and obligations of the relying parties.

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

## 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 Certification Authority 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 Relied Roles and Personnel" of this CPS, and Cybertrust Japan Policy Authority（"CTJ PA"） approve this CPS.

### 1.3.2 Registration Authority

The Registration Authority is operated by Cybertrust, and accepts applications for certificates from the Subordinate CA, and screens the applications based on this CPS. Based on the screening results, the Registration Authority instructs the Issuing Authority to issue or revoke the certificates, or dismisses the applications. Cybertrust shall not delegate the performance of RA.
Note that, as described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA.

### 1.3.3 Issuing Authority

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

### 1.3.4 Subordinate CA

The Subordinate CA is a Subordinate CA that was certified by the Certification Authority, and issues and revokes certificates of subscribers; provided, however, that, as described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA.

### 1.3.5 Subscribers

A subscriber is an organization that files an application for a subscriber certificate with the Subordinate CA of the Certification Authority and uses the subscriber certificate issued by the Subordinate CA based on rules and the like to be set forth by the Certification Authority in the future; provided, however, that, as described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA. Thus, under this CPS Version 1.5, the Subordinate CA will also not issue/revoke subscriber certificates.

### 1.3.6 Relying Parties

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

### 1.3.7 Other Relevant Parties

Not applicable.

## 1.4 Certificate Usage

### 1.4.1 Types of Certificates

#### 1.4.1.1 Certification Authority Certificate

The certificate shown in Appendix B of this CPS is a Certification Authority certificate.

#### 1.4.1.2 Certificate (Subordinate CA Certificate)

A Subordinate CA certificate certifies the Certification Authority of the Subordinate CA Operator that issues subscriber certificates; provided, however, that, as described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not issue certificates based on applications of the Subordinate CA.

#### 1.4.1.3 OCSP Server Certificate

OCSP server certificate is a certificate for OCSP that the Certification Authority issues and uses. OCSP server certificate appends the digital signature to OCSP responses when the Certification Authority provides revocation information with regard to the Subordinate CA based on OCSP.

### 1.4.2 Appropriate Certificate Usage

A Subordinate CA certificate is used for certifying the Subordinate CA of the Certification Authority, and must be used as a certification authority certificate.

OCSP server certificate must be used as a certificate that appends the digital signature to OCSP responses when the Certification Authority provides revocation information with regard to the Subordinate CA.

### 1.4.3 Prohibited Certificate Usage

The Certification Authority prohibits the use of certificates for any purpose other than as set forth in "1.4.2 Appropriate Certificate Usage" of this CPS.

## 1.5 Policy Administration

### 1.5.1 Organization to Control Documents

This CPS will be controlled by the Certification Authority.

### 1.5.2 Contact Point

The Certification Authority will accept inquiries related to this CPS and other related matters at the following contact information.

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

| Contact Information |
| --- |
| Cybertrust Japan Co., Ltd., JCSI Root Support<br>Address: Ark Mori Bldg. 30F, 1-12-32 Akasaka, Minato-ku, Tokyo 107-6030<br>Email Address: jcsi-r@cybertrust.ne.jp |

### 1.5.3 Party to Determine Suitability of CPS

Cybertrust will determine the suitability of this CPS.

### 1.5.4 Suitability Approval Procedures

The suitability of this CPS will be 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 Organization to Operate Repositories

Repositories of the Certification Authority will be controlled by Cybertrust.

## 2.2 Information to be Published

The Certification Authority will publish the repositories as follows.

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

- this CPS

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

- CRL issued by the Certification Authority

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

- Certification Authority certificate

## 2.3 Timing and Frequency of Publication

The timing and frequency of publication regarding the information to be published by the Certification Authority shall be as follows; save for cases where repository maintenance or the like is required, but 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 Issue Cycle" of this CPS and the published; and

(iv) the Certification Authority certificate shall be published at least during the operation period of this Certification Authority.

## 2.4 Access Control on Repositories

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

# 3. Identification and Authentication

As described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not issue/revoke certificates based on applications of the Subordinate CA. Thus, under this CPS Version 1.5, the Subordinate CA will also not issue/revoke subscriber certificates. Therefore, the respective items with regard to the subscriber certificates in this Chapter will not be prescribed in this CPS Version 1.5. Cybertrust will separately prescribe the respective items of this Chapter upon commencing the issuance/revocation of certificates.

Notwithstanding the foregoing, it should be noted that the Certification Authority will include the following in Chapter 3.2.2 of this CPS as validation procedure of the Applicant's Organization and Domain Identity upon commencing the issuance/revocation of certificates. And the Certification Authority will also include the following in Chapter 3.2.3, 3.2.5 and 3.2.6 of this CPS.

## 3.2 Initial identity validation

### 3.2.2 Authentication of Organization and Domain Identity

#### 3.2.2.1 Identity

Upon verifying the subscriber, the Subordinate CA shall use public documents and data, documents and data provided by a third party that is deemed reliable by the Subordinate CA, 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 Authority shall visit the subscriber and conduct an on-site survey as needed.

#### 3.2.2.2 DBA/Tradename

The Subordinate CA does not allow DBA / Tradename to be included in subscriber certificate.

#### 3.2.2.3 Verification of Country

The Subordinate CA confirms 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 Subordinate CA validate the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures permitted by the Baseline Requirements, including blow.

And the Subordinate CA will 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 Subordinate CA shall confirm the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

(i) The Subordinate CA confirms the Applicant's identity under Baseline Requirements Section 3.2.2.1 and the authority of the Applicant Representative under Baseline Requirements Section 3.2.5, OR

(ii) The Subordinate CA confirms the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR

(iii) The Subordinate CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note that this method shall not be used on or after August 1, 2018.

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

The Subordinate CA 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 Subordinate CA 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 Subordinate CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re‐use 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.

#### 3.2.2.4.3 Phone Contact with Domain Contact

The Subordinate CA 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 Subordinate CA 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.

#### 3.2.2.4.4 Constructed Email to Domain Contact

The Subordinate CA 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 re‐use 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.

#### 3.2.2.4.5 Domain Authorization Document

The Subordinate CA shall confirm the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Subscriber Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The Subordinate CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

Note that this method shall not be used on or after August 1, 2018.

#### 3.2.2.4.6 Agreed‐Upon Change to Website

The Subordinate CA shall confirm the Applicant's control over the FQDN by confirming one of the following under the "/.wellknown/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 Subordinate CA 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 Request 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 Subordinate CA 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 Subscriber Certificate request, the timeframe permitted for reuse of validated information relevant to the Subscriber Certificate (such as in Section 4.2.1 of Baseline Requirements or Section 11.14.3 of the EV Guidelines).

#### 3.2.2.4.7 DNS Change

The Subordinate CA 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 Subordinate CA SHALL provide a Random Value unique to the Subscriber Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Subscriber Certificate request, the timeframe permitted for reuse of validated information relevant to the Subscriber Certificate (such as in Section 3.3.1 of Baseline Requirements or Section 11.14.3 of the EV Guidelines).

#### 3.2.2.4.8 IP Address

The Subordinate CA shall confirm the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

#### 3.2.2.4.9 Test Certificate

The Subordinate CA does not adopt this method.

#### 3.2.2.4.10 TLS Using a Random Number

The Subordinate CA does not adopt this method.

### 3.2.2.5 Authentication for an IP Address

For each IP Address listed in a Subscriber Certificate, the Subordinate CA SHALL confirm that, as of the date the Subscriber Certificate was issued, the Applicant has control over the IP Address by:

(i) Having the Applicant demonstrate practical control over the IP Address by making an agreed‐upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address;

(ii) Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);

(iii) Performing a reverse‐IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.2.4.

#### 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 determines 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 Section 3.2.2.6 of Baseline Requirements.

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.

#### 3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the Subordinate CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The Subordinate CA SHOULD 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 Subordinate CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

### 3.2.3 Authentication of Individual Identity

Not applicable.

### 3.2.5 Verification of Application Supervisor

The request is verified using a Reliable Method of Communication, in accordance with section 3.2.5 of the Baseline Requirements.

### 3.2.6 Interoperability Standards

Not applicable.

# 4. Certificate Life-Cycle Operational Requirements

As described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA. Thus, under this CPS Version 1.5, the Subordinate CA will also not issue/revoke subscriber certificates. Therefore, the respective statements with regard to the issuance/revocation of the subscriber certificates, more specifically from "4.1 Certificate Application" to "4.8 Change of Certificate", certain statements of "4.9 Certificate Revocation and Suspension" and the respective statements of "4.12 Third Party Deposit of Key and Key Recovery" of this CPS described below, the Certification Authority will separately prescribe the respective items of this Chapter upon commencing the issuance/revocation of certificates.

Notwithstanding the foregoing, it should be noted that the Certification Authority will include the following in Chapter 4.1, 4.2, 4.3.1, 4.9 and 4.10 of this CPS upon commencing the issuance/revocation of certificates.

## 4.1 Certificate Application

### 4.1.1 Persons Who May Apply for Certificates

Either the Applicant or an individual authorized to request Subscriber Certificates on behalf of the Applicant may submit subscriber certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to Subordinate CA.

### 4.1.2 Enrolment Process and Responsibilities

A subscriber shall apply for a Subscriber Certificate upon accepting this CPS and the subscriber agreement. Upon filing an application, a subscriber is responsible for providing true and accurate information to the Subordinate CA.

The method of applying for a subscriber certificate will be posted on Cybertrust's website.

## 4.2 Certificate Application Processing

### 4.2.1 Identity Validation and Execution of Certification Operations

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

### 4.2.2 Approval or Rejection of Certificate Application

The Subordinate CA rejects any subscriber certificate application that the Subordinate CA cannot verify. The Subordinate CA may also reject a subscriber certificate application if the Subordinate CA believes that issuing the Subscriber Certificate could damage or diminish the Subordinate CA’s reputation or business.

If the subscriber certificate application is not rejected and is successfully validated, The Subordinate CA will approve the subscriber certificate application and issue the Subscriber Certificate. The Subordinate CA is not liable for any rejected Subscriber Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Subscriber Certificate’s contents for accuracy prior to using the subscriber certificate.

## 4.3 Certificate Issuance

### 4.3.1 Certificate Issuance Procedures by Certification Authority

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

## 4.4 Certificate Acceptance

Not applicable.

## 4.5 Key Pair and Certificate Usage

Not applicable.

## 4.6 Certificate Renewal Not Involving Key Renewal

Not applicable.

## 4.7 Certificate Re-Key

Not applicable.

## 4.8 Modification of Certificate

Not applicable.

## 4.9 Certificate Revocation and Suspension

### 4.9.1 Circumstance for Revocation

#### 4.9.1.1 Reasons for Revoking a Subscriber Certificate

After issuing subscriber certificates, the issuing Subordinate CA will revoke the target subscriber 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 subscriber 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 Subscriber Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

(iv) The Subordinate CA obtains evidence that the Subscriber Certificate was misused;

(v) The Subordinate CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

(vi) The Subordinate CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Subscriber Certificate is no longer legally permitted;

(vii) The Subordinate CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

(viii) The Subordinate CA is made aware of a material change in the information contained in the Subscriber Certificate;

(ix) The Subordinate CA is made aware that the Subscriber Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

(x) The Subordinate CA determines that any of the information appearing in the Subscriber Certificate is inaccurate or misleading;

(xi) The Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Subscriber Certificate;

(xii) The Subordinate CA's right to issue Subscriber Certificates under these Requirements expires or is revoked or terminated, unless the Subordinate CA has made arrangements to continue maintaining the CRL/OCSP Repository;

(xiii) The Subordinate CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Subscriber Certificate;

(xiv) Revocation is required by the Subordinate CA's Certificate Policy and/or Certification Practice Statement; or

(xv) The technical content or format of the Subscriber Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

#### 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

In the occurrence of the following event, the Certification Authority will revoke the target 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 Certificate Authority that the original subscriber certificate request was not authorized and does not retroactively grant authorization;

(iii) The Certificate Authority 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 Sections 6.1.5 and 6.1.6, ;

(iv) The Certificate Authority obtains evidence that the Subordinate CA Certificate was misused;

(v) The Certificate Authority is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;

(vi) The Certificate Authority determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;

(vii) The Certificate Authority or 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 Certificate Authority's or 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 is required by the Certificate Authority's Certificate Policy and/or Certification Practice Statement; or

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

#### 4.9.1.3 Reason of Revocation Other certificates

(1) Certification Authority Certificate

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

(i) when it is learned that the private key of the Certification Authority has been compromised; or

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

(2) OCSP server Certificate

In the occurrence of any of the following events, the Certification Authority will revoke the corresponding OCSP server certificate at the time that such event is discovered; provided, however, that, with regard to (ii) below, the Certification Authority may revoke the certificate on a day that is separately notified by the Certification Authority before termination of operations:

(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 Persons Eligible for Applying for Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber, may request revocation of a Subscriber Certificate. Third parties may request subscriber certificate revocation for problems related to fraud, misuse, or compromise. Subscriber Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

### 4.9.3 Revocation Application Procedures

A subscriber shall submit a revocation request via a website provided by Cybertrust or email. The revocation request must include information that is known only to the Subordinate CA that issued subscriber certificates and the subscriber, reason of revocation, contact information and so on in accordance with instructions of the Subordinate CA. The Subordinate CA 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 Grace Period up to Revocation Application

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

### 4.9.5 Time Required for Certification Authority to Process Revocation

The Certification Authority will accept the revocation request 24/7.

The Registration Authority of the Certification Authority shall receive the revocation request, take the procedures based on the provisions of "4.9.3 Revocation Request Procedures" of this CPS, and thereafter promptly instruct the Issuing Authority to revoke the target Subscriber Certificate. After receiving the revocation instruction, the Issuing Authority shall promptly revoke the relevant Subscriber Certificate.

### 4.9.6 Revocation Confirmation Method by Relying Parties

The relying parties shall confirm the certificate revocation of the Subordinate CA with the CRL issued by the Certification Authority or the OCSP server.

### 4.9.7 CRL Issue Cycle

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

The Certification Authority 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 Revocation Other certificates" of this CPS or once a year at least.

### 4.9.8 Maximum Delay Time up to CRL Publication

The Certification Authority shall promptly publish the repositories after publishing the CRL.

### 4.9.9 Online Confirmation of Revocation Information

OCSP responses conform to RFC 6960.

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

The OCSP signing Certificate contains the extension of type id-pkix-ocsp-nocheck.

### 4.9.10 Online Certificate Revocation/Status Checking

The Certificate Authority supports an OCSP capability using the GET method.

The Subordinate CA shall provide revocation information based on OCSP, in addition to CRL. The Subordinate CA shall renew the OCSP response, which has a valid term of 240 hours, in a cycle of less than 24 hours.

The Certification Authority shall not provide certificate revocation information with regard to the Subordinate CA based on OCSP.

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 URL to accept OCSP requests shall be as follows;

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

### 4.9.11 Means for Providing Other Forms of Revocation Advertisements

Not applicable.

### 4.9.12 Special Requirements on Compromise of Key

#### 4.9.12.1 Certification Authority Certificate

When the Certification Authority learns that the private key of the Certification Authority has been compromised, the Certification Authority shall take the revocation procedures of the Certification Authority certificate based on "4.9.3 Revocation Application Procedures" of this CPS.

#### 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 Revocation Application Procedures" of this CPS.

### 4.9.13 Certificate Suspension Requirements

Not applicable.

### 4.9.14 Persons Eligible for Applying for Suspension

Not applicable.

### 4.9.15 Suspension Application Procedures

Not applicable.

### 4.9.16 Term of Suspension

Not applicable.

## 4.10 Certificate Status Services

### 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 Certificate Authority shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

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

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

## 4.11 End of Subscription (Registration)

Not applicable.

## 4.12 Key Escrow and Recovery

Not applicable.

# 5. Management, Operational, And Physical Controls

## 5.1 Physical Security Construction

### 5.1.1 Site Location and Structure

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 "5.1.9 off-site backup " of this CPS). The Facility shall undergo architectural measures for preventing earthquakes, fires, floods and other disasters as well as preventing unauthorized invasion. Information regarding the location of the Certification Authority shall not be indicated outside or inside the building where the Facility is located.

### 5.1.2 Physical Access

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

The Facility and the respective rooms where certification operations are performed in the Facility shall be monitored with a monitoring system 24/7.

### 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 Control Measures

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 Control Measures

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 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.

### 5.1.7 Medium Storage Site

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.

### 5.1.8 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.

### 5.1.9 Off-site Backup

The original or copy of the private key of the Certification Authority 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.

## 5.2 Procedural Controls

### 5.2.1 Relied Roles and Personnel

The Certification Authority shall set forth the personnel required for operating the Certification Authority (the "Certification Authority Staff") and their roles as follows.
However, as described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not issue/revoke the Subordinate CA certificate or issue/revoke the subscriber certificate through the Subordinate CA. Thus, the Certification Authority Staff related to the Registration Authority (Registration Authority Manager, Registration Authority Operator Manager, and Registration Authority Operator set forth below) is not appointed. The Certification Authority Staff related to the Registration Authority shall be separately appointed upon commencing the issuance/revocation of certificates.

#### 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 from the Subordinate CA 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 Personnel Required for Each Role

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

### 5.2.3 Personal Identification and Verification of Each Role

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

### 5.2.4 Roles Requiring Segregation of Duties

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

## 5.3 Personnel Security Controls

### 5.3.1 Qualifications, Experience, Clearances

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 Checks and Clearance 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 Authority shall implement training requirements and procedures to all employees who will be assigned as the Certification Authority Staff. The training requirements and procedures shall include, in addition to the education of this CPS, 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 Period and Procedures

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

(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 Frequency and Sequence for Job Rotation

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

### 5.3.6 Sanction against 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 Contract Requirements of Contract Employees

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 Documents Available to Certification Authority Staff

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

## 5.4 Audit Logging Procedures

### 5.4.1 Types of Events to be Recorded

In order to evaluate the compliance of this CPS and the suitability of security, the Certification Authority shall collect the following records as monitoring logs. The records shall include the date and time, subject of the record, and description of event.
However, the records of (i) and (ii) below involving the Registration Authority shall be separately recorded after the issuance/revocation of certificates is commenced based on applications of the Subordinate CA:

(i) records of screenings performed by the Registration Authority;

(ii) records of systems that are being maintained and controlled by the Registration Authority and the Issuing Authority;

(iii) records regarding the entry/exit of the Facility; and

(iv) records regarding the maintenance and control of the Facility.

### 5.4.2 Audit Logging Frequency

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

### 5.4.3 Audit Log Archival Period

Records of the screening performed by the Registration Authority shall be archived at least 7 years after the expiration of the effective period of the certificate that was issued based on the foregoing screening or during the operation period of this Certification Authority, whichever comes first.

Other records shall be archived at least 7 years.

When the monitoring logs are no longer required, the Certification Authority shall dispose such monitoring logs based on the provisions of "5.1.8 Waste Disposal" of this CPS.

### 5.4.4 Audit Log Protection

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

### 5.4.5 Audit Log Backup Procedures

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

### 5.4.6 Audit Log Collection 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 Parties

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

### 5.4.8 Vulnerability Assessment

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 Authority (The OCSP server of the Certification Authority 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 Records to be Archived

The Certification Authority shall archive the following information in addition to the monitoring logs prescribed in "5.4.1 Types of Events to be Recorded" of this CPS.
However, (ii) and (vi) below shall be separately recorded after the issuance/revocation of certificates is commenced based on applications of the Subordinate CA:

(i) Certification Authority certificate;

(ii) Subordinate CA certificate;

(iii) CRL;

(iv) internal audit report;

(v) external audit report;

(vi) application forms and data received from the Subordinate CA; and

(vii) this CPS.

### 5.5.2 Record Archival Period

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

When records are no longer required, the Certification Authority shall dispose such records based on the provisions of "5.1.8 Waste Disposal" of this CPS.

### 5.5.3 Record Protection

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

### 5.5.4 Record Backup Procedures

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

### 5.5.5 Time-stamping

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

### 5.5.6 Record 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 Record Acquisition and Verification Procedures

The Certification Authority 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 Change Over of Certification Authority

Not applicable.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Compromise and Disaster Recovery Procedures

When the Certification Authority learns that the private key of the Certification Authority has been compromised, the Certification Authority shall execute the following, and simultaneously notify the fact of such compromise to the browser vendor that has registered the Certification Authority 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 Certification Authority; 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 Certification Authority suffers from a disaster, the Certification Authority shall perform recovery operations of backup key information and data based on the business continuation plan prescribed in "5.7.4 Business Continuity upon Disasters" 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 Procedures upon System Resource Failure

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

### 5.7.3 Procedures upon Compromise of Subscriber Private Key

As described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not issue/revoke certificates based on applications of the Subordinate CA. Accordingly; procedures to be taken when the private key of the Subordinate CA is compromised are not prescribed. These procedures shall be separately appointed upon commencing the issuance/revocation of certificates.

### 5.7.4 Business Continuity upon Disasters

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

## 5.8 Termination of Certification Authority Operations

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

# 6. Technical Security Controls

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

The key pair used in the Certification Authority 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 PUB 140-2 Level 3 for managing the key pair of the Certification Authority, 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 Certification Authority shall be transferred in the presence of the auditor set forth in "8.2 Auditor Requirements" and "8.3 Relation of Auditor and Auditee" of this CPS or, when the auditor is not available, by presenting to the auditor the transfer records and the recording of the key confirmation procedures so as to ensure that the transfer of the key pair of the Certification Authority was performed according to predetermined procedures.

The key pair of an OCSP server 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, the HSM that satisfies the standards of FIPS PUB 140-2 Level 3 will be used.

### 6.1.2 Delivery of Subscriber Private Key

As described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA. Thus, under this CPS Version 1.5, the Subordinate CA will also not issue/revoke subscriber certificates. Therefore, matters regarding the delivery of the subscriber private key will not be prescribed. The Certification Authority will separately prescribe matters regarding the delivery of private keys of the Subordinate CA and subscribers upon commencing the issuance/revocation of certificates.

### 6.1.3 Delivery of Subscriber Public Key to Certification Authority

As described in "1.1 Overview" of this CPS, under this CPS Version 1.5, the Certification Authority will not perform the procedure of issuance/revocation of certificates based on applications of the Subordinate CA. Thus, under this CPS Version 1.5, the Subordinate CA will also not issue/revoke subscriber certificates. Therefore, matters regarding the delivery of the subscriber public key to the Certification Authority will not be prescribed. The Certification Authority will separately prescribe matters regarding the delivery of the subscriber public key to the Certification Authority upon commencing the issuance/revocation of certificates.

### 6.1.4 Delivery of Certification Authority Public Key to Relying Parties

The Certification Authority will not deliver the public key of the Certification Authority to relying parties. The Certification Authority certificate including the public key of the Certification Authority will be published in the repositories of the Certification Authority.

### 6.1.5 Key Length

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

| Certification Authority Name | Signature Algorithm | Key Length |
|---|---|---|
| SecureSign RootCA11 | SHA1 with RSA | 2048 bit |

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 | SHA2 with RSA | 2048 bit |

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

| Subordinate CA Certificate | Signature Algorithm | Key Length |
|---|---|---|
| Subordinate CA certificate issued by SecureSign RootCA11 | SHA2 with RSA | 2048 bit |

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 |

### 6.1.6 Generation and Check of Public Key Parameter

The Certificate Authority 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

The key usage of the Certification Authority certificate shall be Certificate Signing, CRL Signing.

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

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance as described below.

### 6.2.1 Cryptographic Module Standards and Controls

The cryptographic module for controlling the key pair of the Certification Authority shall be the HSM that satisfies the FIPS PUB 140-2 Level 3 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 Controls by Multiple Persons

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

### 6.2.3 Private Key Escrow

The Certification Authority and the OCSP server will not escrow the private key used by the Certification Authority.

### 6.2.4 Private Key Backup

The Issuing Authority System Administrator shall back up the private key of the Certification Authority. 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 Issuing Authority System Administrator shall back up and store the private key used by the OCSP server in an encrypted state.

### 6.2.5 Private Key Archive

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

### 6.2.6 Private Key Transfer

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

The Certification Authority transfer 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 it is necessary to restore the private key of an OCSP server certificate, the Issuing Authority System Certification Authority shall restore the private key using the system backup in the main site; provided, however, that, based on the approval of the Certification Authority Supervisor, there may be cases where the corresponding OCSP server certificate is revoked and a private key is newly generated.

### 6.2.7 Private Key Storage in Cryptographic Module

The private key of the Certification Authority and the OCSP server shall be stored in the HSM that satisfies the standards of FIPS PUB 140-2 Level 3.

### 6.2.8 Private Key Activation

The private key used by the Certification Authority and the OCSP server 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 Private Key Deactivation

The private key used by the Certification Authority and the OCSP server 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 Private Key Destruction

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 Assessment

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

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Storage of Public Key

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 Certification Authority shall be as follows.

| Key Pair | Validity Period |
|---|---|
| Key Pair of Certification Authority | April 8, 2029 |

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

| Certificate | Validity Period |
|---|---|
| OCSP Server Certificate | Within 25 months |

Upon commencing the issuance of certificates below as a subscriber certificate issued under the Subordinate CA, the validity period of the key pair of the foregoing certificate shall be as follows.

| Certificate | Validity Period |
|---|---|
| OV SSL Certificate | Within 825 days |

## 6.4 Activation Data

### 6.4.1 Creation and Setting of Activation Data

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

### 6.4.2 Activation Data Protection and Controls

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

## 6.5 Computer Security Controls

### 6.5.1 Technical Requirements of Computer Security

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 Assessment

The Certification Authority shall implement, in advance, installation assessment of hardware and software to be installed by the Certification Authority. The Certification Authority 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 Security 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 Authority 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 Authority 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 Certification Authority system shall not be connected to a network, and shall be operated offline.

The OCSP server system of the Certification Authority 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 Time-stamping

According to "5.5.5 Time-stamping" of this CPS.

# 7. Certificate, CRL and OSCP Profiles

## 7.1 Certificate Profile

### 7.1.1 Version No.

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

### 7.1.2 Certificate Extensions

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

### 7.1.3 Algorithm Object Identifier

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

### 7.1.4 Name Format

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

### 7.1.5 Name Restrictions

Not applicable.

### 7.1.6 Certificate Policy Object Identifier

As prescribed in "1.2 Document Name and Identification" of this CPS.

### 7.1.7 Use of Policy Constraint Extensions

Not applicable.

### 7.1.8 Construction and Meaning of Policy Modifier

Not applicable.

### 7.1.9 Processing Method of Certificate Policy Extensions

Not applicable.

## 7.2 CRL Profile

### 7.2.1 Version No.

Matters regarding the CRL of the Certification Authority are set forth in Appendix B.

### 7.2.2 CRL, CRL Entry Extension

Matters regarding the CRL of the Certification Authority are set forth in Appendix B.

## 7.3 OCSP Profile

### 7.3.1 Version No.

Matters regarding an OCSP server certificate of the Certification Authority are set forth in Appendix B.

### 7.3.2 OCSP Extension

Matters regarding an OCSP server certificate of the Certification Authority are set forth in Appendix B.

# 8. Compliance Audit And Other Assessment

The Certification Authority shall at all times:

(i) Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates;

(ii) Comply with these Requirements; and

(iii) Comply with the audit requirements set forth below.

## 8.1 Audit Frequency and Requirements

The Certification Authority verify 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 Auditor Requirements" of this CPS.

## 8.2 Auditor Requirements

A qualified outside 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.

## 8.3 Relation of Auditor and Auditee

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

## 8.4 Scope of Audit

The scope of audit 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.

## 8.5 Measures against Identified Matters

Identified matters that are discovered in the verification will 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 Disclosure of Audit 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 will 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 Baseline Requirements 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

Not applicable.

## 9.2 Financial Responsibility

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

## 9.3 Confidentiality of Business Information

### 9.3.1 Scope of Confidential Information

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

(i) information set forth in "9.4.2 Information Handled as Personal Information" of this CPS;

(ii) inquiry information received from a third party (including relying parties);

(iii) information relating to the security of the Certification Authority; and

(iv) application information from a subscriber, however, it does not occur in this CPS Version 1.5.

### 9.3.2 Information Outside Scope of Confidential Information

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

(i) information set forth as in "2.2 Information to be Published" of this CPS as information to be published;

(ii) information which became public knowledge due to reasons other than the negligence on the part of the Certification Authority;

(iii) information which became public knowledge without any restriction of confidentiality from a party other than the Certification Authority;

(iv) information for which the other party agreed in advance to the effect of being disclosed or provided to a third party; and

(v) application information from a subscriber, however, it does not occur in this CPS Version 1.5.

### 9.3.3 Responsibility of Protecting Confidential Information

The Certification Authority shall take measures for preventing the divulgence of the Confidential Information. The Certification Authority shall not use the Confidential Information for any purpose other than for performing its operations; provided, however, that, when disclosure of the Confidential Information is demanded in the course of judicial, administrative or other legal proceedings; or when the Confidential Information is to be disclosed to a party such as a financial advisor or a potential acquirer/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 Protection of Personal Information" of this CPS.

## 9.4 Protection of Personal Information

### 9.4.1 Privacy Policy

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

### 9.4.2 Information Handled as Personal Information

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

### 9.4.3 Information not Deemed Personal Information

The Certification Authority shall not deem, as personal information, any information other than the information set forth in "9.4.2 Information Handled as Personal Information" of this CPS.

### 9.4.4 Responsibility of Protecting Personal Information

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

### 9.4.5 Notification to and Consent from Individuals on Use of Personal Information

The Certification Authority 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 based on Judicial or Administrative Procedures" of this CPS.

### 9.4.6 Disclosure based on Judicial or Administrative Procedures

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

### 9.4.7 Other Cases of Information Disclosure

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

## 9.5 Intellectual Property Rights

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

(i) this CPS;

(ii) public key and private key of the Certification Authority; and

(iii) certificates issued by the Certification Authority 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.

The representations and warranties of the subscribers will be separately prescribed when the Subordinate CA commences its certification issuance/revocation of the Subscriber Certificate based on the subscriber's application.

### 9.6.1 Representations and Warranties of Issuing Authority

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

(i) to safely control the Certification Authority 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 Authority system; and

(v) to maintain and control the repositories.

Under this CPS Version 1.5, the Certification Authority shall not perform the procedure of issuance/revocation of the Subordinate CA certificate or the subscriber certificate through the Subordinate CA.

### 9.6.2 Representations and Warranties of Registration Authority

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

(i) to accept inquiries ("1.5.2 Contact Point" of this CPS).

Under this CPS Version 1.5, the Certification Authority shall not perform the procedure of issuance/revocation of the Subordinate CA certificate or the subscriber certificate through the Subordinate CA. Accordingly; the Registration Authority shall not screen the Subordinate CA and the subscribers, or process applications for certification issuance/revocation to be filed with the Issuing Authority.

### 9.6.3 Representations and Warranties of Subscribers

Not applicable in this CPS Version 1.5.

Notwithstanding the foregoing, it should be noted that a subscriber represents and warrants that it bears the following obligations upon commencing the issuance/revocation of certificates:

(i) provide true and accurate information upon applying for the issuance of a subscriber certificate;

(ii) comply with the usage of the subscriber certificate;

(iii) refrain from using the subscriber certificate in websites and emails that are contrary to public order and morals;

(iv) refrain from requesting and using a subscriber certificate when any of the items(including metadata) prevented as the organization unit(OU) in section 7.1.4.2.2 of Baseline Requirements are included in the organization unit (OU) of the subscriber certificate

(v) 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;

(vi) strictly manage the private key and password to ensure the confidentiality and safety thereof;

(vii) install a subscriber certificate only in a server that is accessible by the FQDN included in the subscriber certificate, and use the subscriber certificate only for the business acknowledged by Subscriber according to the subscriber agreement;

(viii) in the occurrence of an event set forth in 4.9.1.1 of this CPS, promptly submit an application for the revocation of the subscriber certificate;

(ix) upon determining that the private key has been compromised or there is a possibility thereof, promptly submit an application for the revocation of the subscriber certificate;

(x) refrain from using an expired subscriber certificate or a revoked subscriber certificate; and

(xi) observe applicable laws and regulations.

### 9.6.4 Representations and Warranties of Relying Parties

The relying parties represent and warrant that they bear the following obligations:

(i) to confirm the effective period and entries of the Certification Authority;

(ii) to verify the digital signature and confirm the issuer of the Certification Authority certificate;

(iii) to confirm whether the certificate has been revoked based on CRL or the OCSP server; and

(iv) 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 Authority shall not be liable for any default based on this CPS regarding damages excluding direct damages arising in relation to the warranties set forth in "9.6.1 Representations and Warranties of Issuing Authority" and "9.6.2 Representations and Warranties of Registration Authority" of this CPS.

The Certification Authority 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 Representations and Warranties of Registration Authority" of this CPS:

(i) any damage that arises regardless of the Certification Authority 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 Authority 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 a 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 relying parties or other third parties with regard to any and all damages arising in relation to the use of the Certification Authority certificate 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 Authority shall not be liable for any data loss, indirect damages including lost profits, consequential damages and punitive damages to the extent permitted under the governing law set forth in "9.1.4 Governing Law" of this CPS.

## 9.9 Indemnities

### 9.9.1 Indemnities of CAs

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; or

(ii) breach of this CPS.

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

### 9.9.2 Indemnification by Subscribers

Not applicable.

### 9.9.3 Indemnification by Relying Parties

Not applicable.

## 9.10 Term of Document and Termination

### 9.10.1 Term of Document

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 Certification Authority terminates its operations, excluding the cases prescribed in "9.10.3 Influence of Termination and Surviving Provisions" of this CPS.

### 9.10.3 Influence of Termination and Surviving Provisions

The provisions of9.3, 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

Not applicable.

## 9.12 Amendments

### 9.12.1 Amendment Procedures

The Certification Authority 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 Method and Period

After the CTJ PA approves the amendment of this CPS, the Certification Authority shall take measures to post the CPS before amendment and the CPS after amendment for a given period on the website so that the 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 Change of Object Identifier

Not applicable.

## 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

Not applicable.

## 9.16 Miscellaneous Provisions

### 9.16.1 Entire Agreement

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

### 9.16.2 Assignment of Rights

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 Enforceability

Not applicable.

### 9.16.5 Force Majeure

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

# Appendix A: List of Definitions

| Term | Definition |
|---|---|
| Archive | As used herein, the term "archive" refers to the process of storing expired certificates for a predetermined period. |
| Cryptographic Module | Software, hardware, or a device configured from the combination of such software and hardware that is used for ensuring security in the generation, storage and use of private keys. |
| Suspension | Measure for temporarily invalidating a certificate during the effective period of that certificate. |
| Subordinate CA | Also known as Intermediate CA. Certification Authority that receives the issuance of a Certification Authority certificate from the Root CA, and issues a certificate to the End Entity. |
| 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. |
| 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 organization set forth by Cybertrust that supervise the Certification Authority and review/approve 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. |
| Baseline Requirements | Requirements for issuing publicly-trusted certificates which were formulated by the CA/Browser Forum. |
| Distinguished Name | An identifier set forth in the X.500 recommendation formulated by ITU-T. Configured from attribute information such as a common name, organization name, organizational unit name, and country name. |
| FIPS PUB 140-2 Level 3 | FIPS PUB 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. |
| ITU-T | Telecommunications Standardization Sector of the International Telecommunication Union. |
| OCSP | Abbreviation of "Online Certificate Status Protocol", and is a communication protocol for providing certificate revocation information. |
| 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. |
| 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<br>type：INTEGER<br>value：2 | <br><br>2 (Ver.3) |
| **Serialnumber** | | **value** |
| CertificateSerialNumber | serial number of certificate<br>type：INTEGER<br>value：unique positive integer | <br><br>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)<br>type：OID<br>value：1 2 840 113549 1 1 5 | <br><br>1.2.840.113549.1.1.5 |
| parameters | Parameters of cryptographic algorithm<br>type：NULL<br>value： | <br>NULL |
| **Issuer** | | **value** |
| CountryName | Country-name attribute of certificate issuer | |
| type | Object ID for the country name<br>type：OID<br>value：2 5 4 6 | <br><br>2.5.4.6 |
| value | Value of country name<br>type：PrintableString<br>value：JP | <br><br>JP |
| OrganizationName | Organization-name attribute of certificate issuer | |
| type | Object ID for the organization name<br>type：OID<br>value：2 5 4 10 | <br><br>2.5.4.10 |
| value | Value of organization name<br>type：PrintableString<br>value：Japan Certification Services, Inc. | <br><br>Japan Certification Services, Inc. |
| CommonName | Common-name attribute of certificate issuer | |
| Type | Object ID for the common name<br>type：OID<br>value：2 5 4 3 | <br><br>2.5.4.3 |
| value | Value of common name<br>type：PrintableString<br>value：SecureSign RootCA11 | <br><br>SecureSign RootCA11 |
| **Validity** | | **value** |
| Validity | Validity period of certificate | |
| notBefore | the date on which the certificate validity period begins<br>type：UTCTime<br>value：090408045647Z | <br><br>April 8th 2009, 04:56:47(GMT) |
| notAfter | the date on which the certificate validity period ends<br>type：UTCTime<br>value：290408045647Z | <br><br>April 8th 2029, 04:56:47(GMT) |
| **Subject** | | **value** |
| CountryName | Country-name attribute of certificate subject | |
| type | Object ID for the country name<br>type：OID<br>value：2 5 4 6 | <br><br>2.5.4.6 |
| value | Value of country name | |

| | | |
|---|---|---|
| | type：PrintableString<br>value：JP | <br>JP |
| OrganizationName<br>type | Organization-name attribute of certificate subject<br>Object ID for the organization name<br>type：OID<br>value：2 5 4 10 | <br><br><br>2.5.4.10 |
| value | Value of organization name<br>type：PrintableString<br>value：Japan Certification Services, Inc. | <br><br>Japan Certification Services, Inc. |
| CommonName<br>type | Common-name attribute of certificate subject<br>Object ID for the common name<br>type：OID<br>value：2 5 4 3 | <br><br><br>2.5.4.3 |
| value | Value of common name<br>type：PrintableString<br>value：SecureSign RootCA11 | <br><br>SecureSign RootCA11 |
| **subjectPublicKeyInfo** | | **value** |
| SubjectPublicKeyInfo<br>AlgorithmIdentifier<br>algorithm | Subject's public key information<br>the identifier for the cryptographic algorithm<br>Object ID for the cryptographic algorithm (RSA PUBLIC KEY)<br>type：OID<br>value：1 2 840 113549 1 1 1 | <br><br><br><br>1.2.840.113549.1.1.1 |
| parameters | Parameters of cryptographic algorithm<br>type：NULL<br>value： | <br>NULL |
| subjectPublicKey | Value of public key<br>type：BIT STRING<br>value：public key | <br><br>2048Bit length of public key |

(Expansion Area)

| **subjectKeyIdentifier (extnId :== 2 5 29 14，critical :== FALSE)** | | **value** |
|---|---|---|
| SubjectKeyIdentifier<br>keyIdentifier | Subject Key Identifier<br>the identifier for the public key<br>type：OctetString<br>value：hash of the value of the BIT STRING subjectPublicKey | <br><br><br>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.<br>type：BitString<br>value：000001100 (keyCertSign,cRLSign) | <br><br><br>000001100 |
| **basicConstraints (extnId :== 2 5 29 19，critical :== TRUE)** | | **value** |
| BasicConstraints<br>cA | Basic Constraints<br>The flag to determine whether the supplied certificate is associated with a CA or an end entity<br>type：Boolean<br>value：True (associated with the CA) | <br><br><br><br>TRUE |

CRL

(Standard Area)

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

(Expansion Area)

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

(Entry Area)

| **RevokedCertificates** | | **value** |
|---|---|---|
| CertificateSerialNumber | serial number of revoked certificate<br>type：INTEGER<br>value：unique positive integer | |
| revocationDate | The date on which the revocation occurred<br>type：UTCTime<br>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<br>type：GeneralizedTime<br>value：yyyymmddhhmmssZ | |
| **cRLReason (extnId :== 2 5 29 21, critical :== FALSE)** | | **value** |
| cRLReason | the reason for the certificate revocation<br>type：Enumerated<br>value：reason code for the revocation | |

OCSP Server Certificate

（Standard Area）

| **Version** | | **value** |
|---|---|---|
| Version | Version of the encoded certificate | |

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

| | | |
|---|---|---|
| | issuer | |
| type | Object ID for the common name<br>type：OID | |
| | value：2 5 4 3 | 2.5.4.3 |
| value | Value of common name<br>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)<br>type：OID | |
| | value：1 2 840 113549 1 1 1 | 1.2.840.113549.1.1.1 |
| parameters | Parameters of cryptographic algorithm<br>type：NULL | NULL |
| | value： | |
| subjectPublicKey | Value of public key<br>type：BIT STRING | |
| | value：public key | public key of 2048 bit length |

（Expansion Area）

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