Cybertrust Japan
SureServer Certificate Policy

Version 1.8

Cybertrust Japan Co., Ltd.

November 30, 2021

Revision History

Version	Date	Reason for Revision
1.0	September 27, 2019	Formulation of initial version
1.1	November 27, 2019	- Add section “3.2.2.4.17 Phone Contact with DNS CAA Phone Contact” based on revised Baseline Requirements v1.6.6. - Clarify the description related to revocation request on the application-account-site to section “3.4 Identity Validation and Authentication upon Revocation Request”. - Add the problem report from the third party to section “4.9.2 Persons Who May Request Revocation”. - Add the revocation procedure for the problem report informed by the third party and the procedure of providing the report afterwards to section “4.9.3. Procedure for Revocation Request”. - Add the definitions of terms in Appendix A - Modify typos.
1.2	April 20, 2020	- Modify the title name of each sections to adjust to RFC 3647. - ”1.1 Overview” Clarify types of requirements Cybertrust is compliant with. - Clarify the description of ”1.3.2 Registration Authority". - Added not to issue certificates containing ".onion" in "3.2.2.4 Validation of Domain Authorization or Control". - This Certification Authority ceases using the validation method listed in “3.2.2.4.6 Consistent website change” and starts using “3.2.2.4.18 Consistent website change” newly adopted, after the revision of Baseline Requirements v1.6.8 is effective. - Add description on OCSP stapling in”4.9.11 Other Forms of Revocation Advertisements Available”. - Add the specification of the key parameter in “6.1.6 Public Key Parameters Generation and Quality Checking”. - Add OIDs in “7.1.6 Certificate Policy Object Identifier”. - Minor modifications on phraseology and fix of typos.
1.3	September 1, 2020	- Modify validation requirement when reissuing certificates listed in “3.3.2 Identification and Authentication for Re-key after Revocation”. - Changed the subscriber certificates’ lifetime listed in “6.3.2 Certificate Operational Periods and Key Pair Usage Periods”.
1.4	October 1, 2020	- Add descriptions in “4.9.10 On-line Revocation Checking Requirements” - Add descriptions in "7.1.1 Version Number(s)" - Add descriptions in “7.1.2 Certificate Extensions” - Add descriptiosn in “7.1.3 Algorithm Object Identifiers” - Add descriptions in “7.1.4 Name Forms” - Add descriptions in “7.1.6 Certificate Policy Object Identifier” - Add descriptions in “7.2.1 Version Number(s)” - Modify the description in “8.6 Communication of Results” - Add stipulation on the conditions for certificate re-issuance without charge in “9.1 Fees” - Added a definition in “Appendix A List of Definitions”

1.5	April 1, 2021	- Update the version number of RFC document referenced in "CAA Record (Certification Authority Authorization Record)" - Add descriptions in Section "3.2.2.4 Validation of Domain Authorization or Control" - Modify the description in "4.9.1.1 Reasons for Revoking a Subscriber Certificate" - Modify the description in "5.4.3 Retention Period for Audit Log" - Add generation of subscriber's key pair in "6.1.1 Key Pair Generation" - Add descriptions in Section " 6.1.5 Key Sizes" - Modified the description in Section "7.1.2 Certificate Extensions" - Add descriptions in Section "7.2 CRL Profile" - Add descriptions in Section "7.3 OCSP Profile" - Deleted part of the description of "9.1 Fees" - Modify the description in "9.6.3 Subscriber Representations and Warranties" - Add definitions of terminology in Appendix A - Minor modifications on phraseology and fix of typos
1.6	April 30, 2021	- Add descriptions on reuse of previous validation in Section "3.2.2.4 Validation of Domain Authorization or Control" - Add descriptions on reuse of previous validation in Section"3.2.2.5 Authentication for an IP Address" - Add a revocation reason in Section " 4.9.1.1.2 Reason of Revocation by this Certification Authority" - Add instructions for the problem report regarding a private key compromise in Section " 4.9.12 Special Requirements Related to Key Compromise" - Modify the description in " 7.1.2 Certificate Extensions" - Modify the description in " 8.6 Communication of Results" - Minor modifications on phraseology and fix of typos.
1.7	June 30, 2021	- Modified the acceptable HTTP status code response allowed for redirects listed in "3.2.2.4.18 Agreed‑Upon Change to Website v2" - Modify the instructions for the problem report regarding a private key compromise in Section " 4.9.12 Special Requirements Related to Key Compromise" - Add generation of subscriber's key pair in "6.1.1 Key Pair Generation" - Add definitions of terminology in Appendix A - Minor modifications on phraseology and fix of typos.
1.8	November 30, 2021	- Modify descriptions on the domain name validation in"3.2.2.4.18 Agreed‑Upon Change to Website v2"

*Note
This "Cybertrust Japan SureServer Certificate Policy Version 1.8" of Cybertrust Japan Co., Ltd. basically describes the following matters. However, please note that the following is a reference translation, and the effective statement is the original statement in the Japanese language. Please kindly note that Cybertrust Japan Co., Ltd. does not guarantee the accuracy of this English translation in comparison to the original statement in the Japanese language, and will not be liable in any way for any inconsistency between this English translation and the original statement in the Japanese language. Cybertrust Japan Co., Ltd. may provide the revised English translation with the date of revision for the same version of Cybertrust Japan's "Cybertrust Japan SureServer Certificate Policy." Upon disclosure of the new version of "Cybertrust Japan SureServer Certificate Policy" by Cybertrust Japan Co., Ltd., please stop referring to/using this documentation. Your understanding on above mentioned conditions is requested prior to refer to this documentation.

Contents

1. Introduction

1.1 Overview

Cybertrust Japan Co., Ltd. ("Cybertrust") issues publicly trusted “SureServer certificates (unless separately stipulated herein, "certificates") to the subscribers.

The certificate is an Organizational Validation Certificate for use in certifying servers and network devices upon performing SSL/TLS communication.

Certificates are issued by the certification authority operated by Cybertrust ("Certification Authority"). The Certification Authority has been certified by the Root CA operated by SECOM Trust Systems Co., Ltd. (“SECOM Trust Systems”).

Name of Certification Authority	Cybertrust Japan SureServer CA G4
Serial Number of Certification Authority Certificate	22b9b1630cecb43c2e
Validity Period of Certification Authority Certificate	September 27, 2019 to May 29, 2029
Signature System	SHA2 with RSA
Key Length of Certification Authority	2048 bit
Fingerprint (SHA1)	f695c5b4037ae8eae51ea943a4f54d750e0da609
Fingerprint (SHA256)	0207056d172c80bdfb6dc45be9e5808846078d1e6eef1b6ed70259ab332a64c1
Certificates to be Issued	SureServer Certificate
Root CA	Security Communication RootCA2

The Certification Authority is compliant with the following guidelines and laws and ordinances.

i. Cybertrust Japan SureServer Certificate Policy (This document and hereafter called “this CP.”)
ii. Cybertrust Japan Certification Practice Statement (Hereafter called “CPS.”)
iii. Guidelines, requirements imposed on CAs by the provider of the browser, laws, and regulations which the Certification Authority declares that it complies with in the CPS (They include Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates stipulated by CA/Browser Forum (“BR”).)

If there is any discrepancy between this CP and the CPS, this CP shall prevail. If there is any discrepancy between this CP and the Guidelines, the Guidelines shall prevail.

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

Upon specifying the various requirements in this CP, 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 CP or CPS. Matters that do not apply to the Certification Authority in the respective provisions of this CP provided based on the framework of RFC3647 are indicated as "Not applicable".

1.2 Document Name and Identification

The formal name of this CP shall be “Cybertrust Japan SureServer Certificate Policy.”

This CP and the CPS have specific Object ID’s (OID’s) respectively.

Document Name	OID
Cybertrust Japan SureServer Certificate Policy (this CP)	1.2.392.200081.1.23.1
Cybertrust Japan Certification Practice Statement (CPS)	1.2.392.200081.1.21

1.3 PKI Participants

Cybertrust Japan Policy Authority (“CTJ PA”) determines policies such as this CP and the CPS and appoints the Certification Authority Supervisor.

The following describes the parties related to the certificates issued by the Certification Authority. Each party shall observe the obligations set forth in this CP.

1.3.1 Certification Authority

The Certification Authority set forth in “1.1 Overview" of this CP. The Certification Authority consists of a Registration Authority and an Issuing Authority. The Certification Authority is supervised by the Certification Authority Supervisor set forth in "5.2.1 Trusted Roles" of this CP.

1.3.2 Registration Authority

The Registration Authority is operated by Cybertrust, and accepts applications for certificates from subscribers, and screens the applications based on this CP. Based on the screening results, the Registration Authority instructs the Issuing Authority to issue, revoke the certificates of subscribers, or dismiss the applications. The Certification Authority does not delegate any RA operations including domain control validation to any of third parties.

1.3.3 Issuing Authority

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

1.3.4 Subscribers

A subscriber is an organization or independent contractor that applies for a certificate with the Certification Authority based on this CP and uses the certificate based on this CP, the CPS, and the Subscriber Agreement.

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

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

1.3.5 Relying Parties

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

1.3.6 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificate stipulated in this CP is the Organizational Validation Certificate for SSL/TLS communications. The certificate indicates that the subscriber is an organization that exists and that the Certification Authority certifies that the subscriber has the right to use the Fully-Qualified Domain Name ("FQDN"). It also achieves SSL/TLS encrypted communications between the server device to which the FQDN is assigned and the client devices of the relying parties. Upon issuing a certificate, the Registration Authority shall screen the following matters based on this CP:

i. legal or physical existence of subscribers;
ii. a subscriber has the right to use the FQDN included in the certificate;
iii. the OU attribute listed in the certificates does not include the name, DBA, product name, trademark, address, location, or other text refers to a specific natural person or Legal entity unless the Certification Authority verifies that specified information indicates the Subscriber. This field MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable;
iv. the Application Supervisor works for the organization
v. acceptance of the Subscriber Agreement;
vi. approval of the application supervisor for the procedural manager to submit an application; and
vii. high risk status. (Screening shall be implemented when an application is determined to be high-risk, such as the high risk of phishing or other abuses.)

1.4.2 Prohibited Certificate Uses

The Certification Authority prohibits the use of certificates for any purpose other than as set forth in "1.4.1 Appropriate Certificate Uses" of this CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP and the Subscriber Agreement and the CPS that this CP refers to are administered by Cybertrust, which operates all Certification Authorities.

1.5.2 Contact Person

The Certification Authority accepts inquiries related to the services provided by Cybertrust and this CP at the following contact information.

Contact Information

Cybertrust Japan Co., Ltd. SureServer Section

Address: 13F SE Sapporo Bldg., 1-1-2 Kita 7-jo Nishi, Kita-ku, Sapporo-shi 060-0807

Tel: 0120-957-975 or +81-11-708-5283

Business Days: Monday to Friday (excluding National Holidays, and the designated days addressed on Cybertrust's website including Year-End and New Year)

Business Hours: 9:00 to 18:00

Inquiries and complaints: As indicated below

Description	Address
・Inquiries regarding the application process for issuance and technical inquiries. ・Other inquiries regarding this CP, etc. ・Capable of response from 9:00 to 18:00 on business days.	ss-apply@cybertrust.ne.jp
・Inquiries regarding revocation requests and application process. ・Inquiries regarding problems with certificates or upon discovery of fraudulent certificates. ・Communication of other complaints. ・Capable of response for 24 x7.	evc-report@cybertrust.ne.jp

1.5.3 Person Determining CP Suitability for the Policy

Certificates of the Certification Authority are issued by the Root CA operated by SECOM Trust Systems. This CP must suit the requirements by the Root CA, and the suitability is evaluated and determined by CTJ PA and SECOM Trust Systems.

1.5.4 CP Approval Procedures

The suitability described in "1.5.3 Person Determining CP Suitability for the Policy" of this CP shall go through an external audit, and then be approved by CTJ PA and SECOM Trust Systems.

1.6 Definitions and Acronyms

As prescribed in Appendix A of this CP.

2. Publication and Repository Responsibilities

2.1 Repositories

Repositories of the Certification Authority are controlled by Cybertrust.

2.2 Publication of Certification Information

The Certification Authority publishes the following information in repositories.

i. Publish the following information at https://www.cybertrust.ne.jp/ssl/repository/index.html.

- this CP
- Subscriber Agreement for the certificate
- CPS
- other terms and conditions regarding the services of the certificate (the "Related Rules")

ii. Publish the following information at http://crl.cybertrust.ne.jp/SureServer/ovcag4/cdp.crl.

- CRL issued by the Certification Authority

iii. Publish the following information at https://www.cybertrust.ne.jp/sureserver/support/download_ca.html.

- certificates of the Certification Authority

2.3 Time or Frequency of Publication

The timing and frequency of publication regarding the information to be published by the Certification Authority shall be as follows. This does not apply for the cases where repository maintenance or the like is required, but CRL shall be available 24 hours.

i. this CP, the CPS, the Subscriber Agreement for each certificate, and the Related Rules shall be published each time they are amended;
ii. this CRL shall be renewed according to the cycle prescribed in “4.9.7 CRL Issuance Frequency" of this CP and the published; and
iii. the certificates of the Certification Authority shall be published at least during the effective period.

2.4 Access Controls on Repositories

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

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

3.1.2 Need for Names to Be Meaningful

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

DN Item	Meaning
Common Name	Complete host name of server or network device to use the certificate (FQDN).
Organization	Name of the organization or independent contractor of the subscriber.
Organizational Unit * (optional item)	Department name, service name, shop name (only for an independent contractor). * Any of the values described in "1.4.1 (iii)" of this CP must not be included.
Locality	Address of business location or independent contractor (locality).
State or Province	Address of business location or independent contractor (state or province).
Country	Address of business location or independent contractor (country).

3.1.3 Anonymity or Pseudonymity of Subscribers

This Certification Authority does not accept any certificate request by anonymity or pseudonymity of a subscriber.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

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

3.2.2 Authentication of Organization Identity

3.2.2.1 Identity

The Certification Authority shall verify the matters set forth in "1.4.1 Appropriate Certificate Uses" of this CP.

Upon verifying the subscriber, the Certification Authority shall use public documents and data, the documents and data provided by a third party that is deemed reliable by the Certification Authority, and the documents and data provided by the subscriber, as well as make inquiries to an appropriate individual affiliated with the subscriber or an organization that constitutes the subscriber. The subscriber shall be visited for screening as required.

However, when there are documents or data that were received from the subscriber or documents or data that were independently obtained by the Certification Authority during the period that was posted on the website by Cybertrust or the period notified to the subscriber, and such documents or data have been screened by the Certification Authority and are valid, the Certification Authority shall not request the resubmission of such documents or data.

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

3.2.2.2 DBA/Tradename

When the organization name to be included in the subscriber's certificate is DBA/Tradename, this Certification Authority shall confirm the name by using public documents and data or the documents and data provided by a third party that is deemed reliable by the Certification Authority, based on Section 3.2.2.2 of the BR.

3.2.2.3 Verification of Country

This Certification Authority confirms the Country included in the subscriber's certificate based on "3.2.2.1Identity" of this CP.

3.2.2.4 Validation of Domain Authorization or Control

This Certification Authority shall screen, prior to issuance, the subscriber’s authorization or control of the FQDN or domain name in accordance with Section 3.2.2.4 of the BR.

The Certification Authority validates each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. This Certification Authority does not issue a certificate for a FQDN contains ".onion" as the rightmost label.

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

This Certification Authority SHALL maintain a record of which domain validation method, including relevant BR version number, was used to validate every domain.

Note: FQDNs may be listed in Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permitted Subtrees within the Name Constraints extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This Certification Authority does not use this method.

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

This Certification Authority confirms the Subscriber's authorization or control of the FQDN by sending a Random Value (the "Random Value" defined in the BR, hereafter called "Random Value") via email, fax, SMS, or postal mail and then receiving a confirming response containing the Random Value. The Random Value MUST be sent to the 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.

This Certification Authority 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.

This Certification Authority MAY resend the email, fax, SMS, or postal mail, including reuse of the Random Value, provided that the communication's content and recipient(s) remain unchanged.

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

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to the application for a wildcard domain name.

3.2.2.4.3 Phone Contact with Domain Contact

The Certification Authority SHALL NOT perform screening using this method after May 31, 2019. However, completed validations using this method before the date SHALL continue to be valid during the applicable certificate data reuse periods.

This Certification Authority MUST use the phone number identified as the Domain Name Owner's Contact by the Domain Name Registrar to make a call to the Domain Name Owner to examine about the Subscriber's authorization or control of the FQDN.

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

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to the application for a wildcard domain name.

3.2.2.4.4 Constructed Email to Domain Contact

The Certification Authority send emails to one or more email addresses of 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at sign ("@") and the Authorization Domain Name. The emails contain a Random Value. The subscriber's authorization or control of the FQDN is examined by receiving a response containing the Random Value.

If the Authorization Domain Name used in the email address is the Authorization Domain Name for multiple FQDNs, each email MAY confirm the authorization or control of the multiple FQDNs.

The Random Value SHALL be unique in each email.

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

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

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to the application for a wildcard domain name.

3.2.2.4.5 Domain Authorization Document

This Certification Authority does not use this method.

3.2.2.4.6 Agreed-Upon Change to Website

The Certification Authority SHALL NOT perform screening using this method after June 3, 2020. However, completed validations using this method before the date SHALL continue to be valid during the applicable certificate data reuse periods.

Under the "/.well-known/pki-validation" directory or in another path registered with IANA for the purpose of Domain Name Validation via HTTP/HTTPS over an Authorized Port, this Certification Authority confirms the Authorization Domain Name that is accessible and screens the Subscriber's authorization or control of the FQDN.

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,
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, this Certification Authority SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after 30 days or the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of the BR) if the Subscriber submitted a Certificate request.

This certification authority does not adopt Request Token.

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name.

3.2.2.4.7 DNS Change

This Certification Authority SHALL examine the Subscriber's authorization or control of 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 an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

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

This certification authority does not adopt Request Token.

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name.

3.2.2.4.8 IP Address

This Certification Authority shall examine the Subscriber's authorization or control of the domain name by confirming that the Subscriber 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 of the BR.

Note: If the FQDN has been validated using this method, this Certification Authority MAY NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation using an authorized method. This rule does not apply to the screening of a wildcard domain name.

3.2.2.4.9 Test Certificate

This Certification Authority does not use this method.

3.2.2.4.10 TLS Using a Random Number

This Certification Authority does not use this method.

3.2.2.4.11 Any Other Method

This Certification Authority does not use this method.

3.2.2.4.12 Validating Applicant as a Domain Contact

This Certification Authority does not use this method.

3.2.2.4.13 Email to DNS CAA Contact

This Certification Authority SHALL examine the Subscriber's authorization or control of the FQDN by sending a Random Value via email to the email address that can be verified as the DNS CAA Email Contact and then receiving a confirming response containing the Random Value.

The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

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 the email’s entire contents and recipient SHALL remain unchanged.

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

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name.

3.2.2.4.14 Email to DNS TXT Contact

This Certification Authority SHALL examine the Subscriber's authorization or control of the FQDN by sending a Random Value via email to the email address contact in the DNS TXT record (DNS TXT Record Email Contact) and then receiving a confirming response containing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

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 the email's entire contents and recipient SHALL remain unchanged.

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

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name.

3.2.2.4.15 Phone Contact with Domain Contact

This Certification Authority Shall examine the Subscriber's authorization or control of the FQDN by calling the Domain Contact's phone number.

Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same Domain Contact phone number is listed for each Authorization Domain Name being examined and they provide a confirming response for each Authorization Domain Name.

In the event that someone other than a Domain Contact is reached, the Certification Authority MAY request to be transferred to the Domain Contact. In the event of reaching voicemail, the Certification Authority may leave the Random Value and the Authorization Domain Name(s) being examined. The Random Value MUST be returned to the CA to approve the request.

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

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue the subscriber's Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to the application for a wildcard domain name.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

This Certification Authority SHALL examine the Subscriber's authorization or control of the FQDN by calling the contact's phone number (DNS TXT Record Phone Contact) in the DNS TXT record.

Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each Authorization Domain Name being examined and they provide a confirming response for each Authorization Domain Name.

The Certification Authority MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, the Certification Authority may leave the Random Value and the Authorization Domain Name(s) being examined.

The Random Value MUST be returned to the Certification Authority to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue the subscriber's Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

This Certification Authority SHALL examine the Subscriber's authorization or control of the FQDN by calling a phone number verified as the DNS CAA Phone Contact.

The relevant CAA Resource Record Set must be found by using the search algorithm defined in RFC 8659.

Each phone call MAY confirm control of multiple Authorization Domain Names provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each Authorization Domain Name.

The Certification Authority MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, the Certification Authority may leave the Random Value and the Authorization Domain Name(s) being examined.

The Random Value MUST be returned to the Certification Authority to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, the Certification Authority MAY also issue the subscriber's Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name.

3.2.2.4.18 Agreed-Upon Change to Website v2

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

i. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and
ii. This Certification Authority MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

i. MUST be located on the Authorization Domain Name,
ii. MUST be located under the "/.well-known/pki-validation" directory,
iii. MUST be retrieved via either the "http" or "https" scheme, and
iv. MUST be accessed over an Authorized Port.

If this Certification Authority follows redirects the following apply:

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

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

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

If a Random Value is used, then:

i. This Certification Authority MUST provide a Random Value unique to the certificate request.
ii. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation.

This certification authority does not adopt Request Token.

Note: For certificates issued before November 30, 2021,Once the FQDN has been validated using this method, the Certification Authority MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This rule also applies to an application for a wildcard domain name. For the certificate issued on or after December 1, 2021 when using this method, the Certification Authority shall validate each of requested FQDNs and shall not issue certificates for the different FQDNs that end with all the labels of the validated FQDNs unless the Certification Authority processes another validation. This rule does not apply to the validation of a wildcard domain name of OV SSL/TLS Certificate.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

This Certification Authority does not use this method.

3.2.2.4.20 TLS Using ALPN

This Certification Authority does not use this method.

3.2.2.5 Authentication for an IP Address

This Certification Authority Shall screen, prior to issuance, the subscriber’s authorization or control of the IP address in accordance with Section 3.2.2.5 of the BR.

The Certification Authority validates each IP address listed in the Certificate using at least one of the methods listed below.

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

This Certification Authority SHALL maintain a record of which validation method, including relevant BR version number, was used to validate every IP address.

Note: The IP address confirmed by Section 3.2.2.5 may be described in the certificate and the subordinate CA certificate via the IP address in the permitted subtree within the name restriction extension as stipulated in Section 7.1.4.2 of the BR. Describing it in the subordinate CA certificate need not be verified via the IP address in the excluded subtree of the name restriction extension.Agreed‑Upon Change to Website

This Certification Authority confirms the IP address that is accessible in the metatag format under the "/.well-known/pki-validation" directory or in another path registered with IANA for the purpose of IP address validation via HTTP/HTTPS over an Authorized Port. It also screens the Subscriber's authorization or control of the IP address by confirming the presence of a Request Token or Random Value.

The Request Token or Request Value MUST NOT appear in the request.

If a Random Value is used, this Certification Authority SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after 30 days or the timeframe permitted for reuse of validated information relevant to the Certificate (see Section 4.2.1 of the BR) if the Subscriber submitted a Certificate request.

This Certification Authority does not adopt Request Token.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

This Certification Authority does not use this method.

3.2.2.5.3 Reverse Address Lookup

This Certification Authority acquires the domain name associated with the IP address via reverse IP lookup of the IP address. It also screens the subscriber's authorization or control of the IP address by using the method allowed in 3.2.2.4 “Authorization of Domains or Screening of Control" of this CP to confirm that the subscriber controls the FQDN.

3.2.2.5.4 Any Other Method

This Certification Authority does not use this method.

3.2.2.5.5 Phone Contact with IP Address Contact

This Certification Authority does not use this method.

3.2.2.5.6 ACME “http-01” method for IP Addresses

This Certification Authority does not use this method.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

This Certification Authority does not use this method.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate that uses a wildcard character (*) in CN or subjectAltName of DNS or type DNS-ID, this Certification Authority determines whether the wildcard character occurs at the position of the "registry control" label or the first label to the left of the "public suffix" (such as "* .com" and "* .co.uk", see Section 8.2 of RFC 6454 for details). Determination of "registry control" shall be based on Section 3.2.2.6 of the BR.

When a wildcard exists immediately to the left of the registry control or public suffix, this Certification Authority refuses issuance unless the appropriate control of the entire domain name space is confirmed.

3.2.2.7 Data Source Accuracy

This Certification Authority evaluates the reliability of the data source used in examination. The evaluation checks the following items such as the accuracy and the resistance to change or falsification.

i. The age of the information provided,
ii. The frequency of updates to the information source,
iii. The provider and purpose of the collected data,
iv. The public accessibility of the data availability, and
v. The relative difficulty in falsifying or altering the data.

Databases maintained by the Certification Authority, its owner, or its affiliated companies must be independent of the Certification Authority. They do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information with the intention of passing the examination of the Certification Authority.

3.2.2.8 CAA Records

The Certification Authority verifies the CAA Record defined in RFC8659 (DNS Certification Authority Authorization (CAA) Resource Record) and section 3.2.2.8 of the BR.

If the CAA record (issue/issuewild) contains any of the values listed in section 4.2.1 of this CP, the Certification Authority recognizes that it is designated as a certification authority that permits issuance of the certificates.

3.2.3 Authentication of Individual Identity

This Certification Authority does not issue a certificate to individual.

3.2.4 Non-verified Subscriber Information

The Certification Authority does not verify the truthfulness and accuracy of the information described in the subscriber's organization unit (OU).

3.2.5 Validation of Authority

The Certification Authority shall verify that the application supervisor works for the subscriber and has the authority to submit a certificate request on behalf of the subscriber. The Certification Authority shall additionally verify that the application supervisor has accepted the Subscriber Agreement and approved the filing of an application by a phone call to the procedural manager or a method that is equivalent to the phone call. The phone number to be used for the phone call shall be a number provided by a third party or in the document and data provided by the subscriber that are deemed reliable by the Certification Authority.

3.2.6 Criteria for Interoperation

The Certification Authority shall not perform interoperations.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The provisions of “3.2 Initial Identity Validation” of this CP shall apply correspondingly.

3.3.2 Identification and Authentication for Re-key after Revocation

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

However, when it is verified that the certificate information included in the CSR and the expiration date of the certificate to be reissued coincide with the originally issued certificate, validation based on "3.2 Initial Identity Validation" of this CP is not performed, and a certificate shall be issued based on the verification of the foregoing coincidence.

3.4 Identification and Authentication for Revocation Request

When the Certification Authority receives a revocation request from a subscriber via email or in the method indicated on Cybertrust’s website, the Certification Authority shall verify the identity of the person who submitted the revocation, that such person is authorized to submit a revocation request, and the reason of revocation. As the verification method, the Certification Authority shall compare the information notified to the Certification Authority upon application for issuance of a certificate and the information only known to the Certification Authority and the subscriber. The revocation request submitted from the application-account-site by the procedural manager is regarded as an authorized request in a same manner. However, the Certification Authority processes the additional verification if necessary.

Upon receiving a revocation request for a certificate of a specific subscriber from other than the subscriber of that certificate, the Certification Authority shall survey the reason of revocation and verify with the subscriber of the certificate if necessary.

The Certification Authority verifies the information described above and revoke the certificate if the revocation reason is found corresponding any of events set forth in the Subscriber Agreement.

The email address to be used for the revocation request is indicated in "1.5.2 Contact Person" of this CP and on Cybertrust's website.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Persons who may apply for a certificate with the Certification Authority shall only be the application supervisor, or a procedural manager who was authorized by the application supervisor submit a certificate request.

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

The Certification Authority's verification of a subscriber's intent to submit a certificate request shall be answered by the application supervisor or by a person in the subscriber organization who is authorized by the application supervisor.

4.1.2 Enrollment Process and Responsibilities

A subscriber shall apply for a certificate upon accepting this CP, the Subscriber Agreement, and the CPS. Upon filing an application, a subscriber is responsible for providing correct and accurate information to the Certification Authority.

The method of applying for a certificate is posted on Cybertrust's website.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The provisions of “3.2 Initial Identity Validation” of this CP shall apply correspondingly. The Registration Authority of the Certification Authority shall perform the procedure.

If the CAA record (issue/issuewild) contains any of the following values, the Certification Authority recognizes that it is designated as a certification authority that permits issuance of the certificates.

cybertrust.ne.jp
cybertrust.co.jp

4.2.2 Approval or Rejection of Certificate Applications

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

When the requirements prescribed in “3.2 Initial Identity Validation" of this CP are not satisfied, the Certification Authority shall dismiss the application for issuing a certificate and reject issuance. In the foregoing case, the Certification Authority shall notify the reason of such rejection to the application supervisor or the procedural manager who submitted the application. The Certification Authority does not return the information and data obtained from the application supervisor or the procedural manager during the application process.

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

After completing the application procedures based on “3.2 Initial Identity Validation" of this CP, the Registration Authority of the Certification Authority shall instruct the Issuing Authority to issue the subscriber's certificate. Simultaneously with issuing the certificate, the Issuing Authority shall send to the subscriber the notice set forth in "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CP.

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Promptly after the certificate is issued, the Certification Authority shall send an email to the email address designated by the subscriber at the time of application to the effect that the certificate has been issued, and the procedures required for the subscriber to accept the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A subscriber shall accept a certificate according to the notified contents recorded in the email sent from the Certification Authority based on the provisions of "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CP. The Certification Authority shall deem that a subscriber has accepted the certificate when the subscriber downloads the certificate from Cybertrust's prescribed website.

4.4.2 Publication of the Certificate by the CA

The Certification Authority does not publish a subscriber's certificate.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Certification Authority does not notify the issuance of the certificate based on the provisions of “4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CP other than to the email address designated by the subscriber.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

A subscriber shall use its private key and certificate only for the usage set forth in “1.4.1 Appropriate Certificate Uses" of this CP and any other usage is not allowed. Moreover, a subscriber's private key and certificate may only be used by the subscriber, and the subscriber must not license the use thereof to a third party. Other obligations of a subscriber regarding the use of its private key and certificate are set forth in "9.6.3 Subscriber Representations and Warranties" of this CP.

4.5.2 Relying Party Public Key and Certificate Usage

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

Other obligations of a relying party regarding the use of a subscriber's public key and certificate are set forth in "9.6.4 Relying Party Representations and Warranties” of this CP.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

The Certification Authority shall accept a renewal request pursuant to the expiration of the validity period of the certificate used by a subscriber.

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

The provisions of “4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CP shall apply correspondingly.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The provisions of “4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.

4.6.6 Publication of the Renewal Certificate by the CA

The provisions of “4.4.2 Publication of the Certificate by the CA" of this CP shall apply correspondingly.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of “4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

The Certification Authority shall accept a renewal request pursuant to the expiration of the validity period of the certificate used by a subscriber.

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

The provisions of “4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CP shall apply correspondingly.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The provisions of “4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.

4.7.6 Publication of the Re-keyed Certificate by the CA

The provisions of “4.4.2 Publication of the Certificate by the CA" of this CP shall apply correspondingly.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

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

If there is any modification to the certificate information, a subscriber must promptly request the revocation of the corresponding certificate to the Certification Authority for revoking the corresponding certificate.

4.8.2 Who may Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

4.9.1.1.1 Reason of Revocation by Subscriber

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

i. a subscriber discovers a certificate that was issued based on an application for issuance that was not approved by the subscriber;
ii. a subscriber learns that its private key has been compromised or there is a possibility thereof;
iii. a subscriber learns of misuse or unauthorized use of its private key or certificate or the possibility thereof;
iv. there is modification to the contents of a subscriber's certificate;
v. a subscriber loses the right to use the FQDN or the IP address included in the certificate;
vi. a subscriber learns the subject information listed in subscriber's certificate is no longer accurate;
vii. a subscriber violates one or more of its material obligations under this CP, the CPS, or the Subscriber Agreement;
viii. a subscriber discovers that the Certificate was not issued in accordance with the relevant requirements of CA/Browser Forum or this CP, the CPS, or the Subscriber Agreement;
ix. a subscriber wishes to cancel the Subscriber Agreement; or

x. a subscriber wishes to request the free reissuance of a certificate set forth in “9.1 Fees" of this CP.

4.9.1.1.2 Reason of Revocation by this Certification Authority

Prior to revoking a Certificate, this Certification Authority verifies the identity and authority of the entity requesting revocation. This Certification Authority shall revoke a Certificate within 24 hours if one or more of the following occurs:

i. The Subscriber requests in writing that this Certification Authority revokes the certificate;
ii. The Subscriber notifies Cybertrust that the original Certificate request had not been authorized and does not retroactively grant authorization;
iii. This Certification Authority obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
iv. The Certification Authority is made aware of a demonstrated or proven method that can easily compute the Subscriber’s Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or
v. This Certification Authority obtains evidence that screening of the authorization or control of the FQDN or the IP address in the subscriber's Certificate should not be relied upon.

This Certification Authority may revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

i. The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the BR;
ii. Cybertrust obtains evidence that the certificate was misused;
iii. a subscriber breaches a material obligation under this CP, the CPS, or the Subscriber Agreement;
iv. Cybertrust confirms any circumstance indicating that use of the FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant’s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
v. Cybertrust confirms that the subscriber's wildcard certificate is used to certify a fraudulent FQDN;
vi. Cybertrust confirms a material change in the information contained in the certificate;
vii. Cybertrust confirms that the Certificate was issued without complying with the applicable requirements set forth by CA/Browser Forum, this CP, the CPS, or the Subscriber Agreement provided that this Certification Authority may issue the qualified Certificate with the validity ends of its stated period in the original certificate without charge;
viii. The Certification Authority determines or confirms that any of the information appearing in the certificate is inaccurate;
ix. The right of this Certification Authority to issue Certificates based on the requirements of CA/Browser Forum expires, is revoked, or is terminated, unless this Certification Authority has made arrangements to continue maintaining the CRL/OCSP (Online Certificate Status Protocol) Repository;
x. Revocation is required by this CP; or
xi. Cybertrust confirms a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise.

This Certification Authority may revoke any Certificate in its sole discretion, including if one or more of the following occurs:

i. The revocation request is confirmed by "3.4 Identification and Authentication for Revocation Request" of this CP;
ii. Either the Subscriber’s or this Certification Authority’s obligations under this CP and the CPS are delayed or prevented by circumstances beyond the party’s reasonable control, including computer or communication failure, and, as a result, information of this Certification Authority, the Subscriber, or the relying party is materially threatened or compromised;
iii. Cybertrust received a lawful and binding order from a government or regulatory body to revoke the Certificate;
iv. This Certification Authority ceased operations and did not arrange for another Certification Authority to provide revocation support for the Certificates;
v. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

vi. The Subscriber was added as a denied party or prohibited person to a blacklist;
vii. The subscriber fails to pay the fee of the Certificate in breach of Cybertrust's prescribed billing conditions;
viii. Cybertrust cancels the Subscriber Agreement with a subscriber based on the Subscriber Agreement; or
ix. This Certification Authority learns, based on reasonable evidence, that the private key of this Certification Authority and/or the Root CA has been compromised or there is a possibility thereof.

4.9.2 Who Can Request Revocation

Persons who may request revocation shall be the application supervisor, the procedural manager, or an agent who is duly authorized by the subscriber and who knows information that was notified by the Certification Authority when the issuance application of the certificate was submitted, which is shared only between the Certification Authority and the subscriber.

Other third parties may submit Certificate Problem Reports informing the Certification Authority of reasonable cause, if exists, to revoke the certificate.

4.9.3 Procedure for Revocation Request

A subscriber shall submit a revocation request via email or in the method indicated by Cybertrust on its website. The email must include information that is known only to the Certification Authority and the subscriber, reason of revocation, contact information and so on in accordance with instructions of the Certification Authority. The Certification Authority shall verify the reason of revocation as prescribed in “3.4 Identification and Authentication for Revocation Request" of this CP.

For the Problem Report informed by a third party, the Certification Authority SHALL investigate the notified issue and SHALL revoke the certificate when the cause is found reasonable.

The Certification Authority does not notify the revocation to the subscriber after revokes the certificate. For revocations that involve the free reissuance of a certificate set forth in “9.1 Fees" of this CP, there may be cases where the notice of revocation is given together with the notice of free reissuance of a certificate.

4.9.4 Revocation Request Grace Period

In the occurrence of an event corresponding to "4.9.1.1 Reason of Revocation" of this CP, a subscriber shall promptly submit a revocation request.

4.9.5 Time within Which CA Must Process the Revocation Request

The Certification Authority accepts 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 Procedure for Revocation Request" of this CP, and thereafter promptly instruct the Issuing Authority to revoke the target certificate. After receiving the revocation instruction, the Issuing Authority shall promptly revoke the relevant certificate.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

The validity period of the Certification Authority's CRL is no more than 240 hours. The Certification Authority shall publish the certificate in the repository no later than one (1) hour after the issuance thereof.

4.9.9 On-line Revocation/Status Checking Availability

The Certification Authority shall provide revocation information based on OCSP, in addition to CRL. The Certification Authority shall renew the OCSP response, which has a validity period of no more than 240 hours, in a cycle of less than 24 hours. OCSP responses of the Certification Authority conform to RFC 6960. OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

4.9.10 On-line Revocation Checking Requirements

This Certification Authority shall provide revocation information based on OCSP, in addition to CRL. The GET method described in RFC6960 and/or RFC5019 shall be supported for the OCSP.

The Certification Authority shall renew the OCSP response, which has a maximum expiration time of 240 hours, in a cycle of no more than 96 hours.

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

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

4.9.11 Other Forms of Revocation Advertisements Available

If the Subscriber Certificate is for a high-traffic FQDN, this Certification Authority MAY rely on stapling, in accordance with [RFC4366], to distribute its OCSP responses. In this case, this Certification Authority ensure that the Subscriber “staples” the OCSP response for the Certificate in its TLS handshake. This Certification Authority SHALL enforce this requirement on the Subscriber through the Subscriber Agreement.

4.9.12 Special Requirements Related to Key Compromise

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

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

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

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

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

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

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

The Certification 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 Certification 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 Certification Authority. The Certification 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 law enforcement authorities or CTJPA, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

The reasons for ending the use of a subscriber's certificate shall be set forth in the Subscriber Agreement. Moreover, if a subscriber wishes to terminate the Subscriber Agreement midway during the validity period of the certificate, the subscriber must submit a certificate revocation request with the Certification Authority based on "4.9.3 Procedure for Revocation Request " of this CP.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Shall be defined in “5.1.1 Site Location and Construction” of the CPS.

5.1.2 Physical Access

Shall be defined in “5.1.2 Physical Access” of the CPS.

5.1.3 Power and Air Conditioning

Shall be defined in “5.1.3 Power and Air Conditioning” of the CPS.

5.1.4 Water Exposures

Shall be defined in “5.1.4 Water Exposures” of the CPS.

5.1.5 Fire Prevention and Protection

Shall be defined in “5.1.5 Fire Prevention and Protection” of the CPS.

5.1.6 Media Storage

Shall be defined in “5.1.6 Media Storage” of the CPS.

5.1.7 Waste Disposal

Shall be defined in “5.1.7 Waste Disposal” of the CPS.

5.1.8 Off-site Backup

Shall be defined in “5.1.8 Off-site Backup” of the CPS.

5.1.9 Anti-earthquake Measures

Shall be defined in “5.1.9 Anti-earthquake Measures” of the CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Shall be defined in “5.2.1 Trusted Roles” of the CPS.

5.2.2 Number of Persons Required Per Task

Shall be defined in “5.2.2 Number of Persons Required Per Task” of the CPS.

5.2.3 Identification and Authentication for Each Role

Shall be defined in “5.2.3 Identification and Authentication for Each Role” of the CPS.

5.2.4 Roles Requiring Separation of Duties

Shall be defined in “5.2.4 Roles Requiring Separation of Duties” of the CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Shall be defined in “5.3.1 Qualifications, Experience, and Clearance Requirements” of the CPS.

5.3.2 Background Check Procedures

Shall be defined in “5.3.2 Background Check Procedures” of the CPS.

5.3.3 Training Requirements

Shall be defined in “5.3.3 Training Requirements” of the CPS.

5.3.4 Retraining Frequency and Requirements

Shall be defined in “5.3.4 Retraining Frequency and Requirements” of the CPS.

5.3.5 Job Rotation Frequency and Sequence

Shall be defined in “5.3.5 Job Rotation Frequency and Sequence” of the CPS.

5.3.6 Sanctions for Unauthorized Actions

Shall be defined in “5.3.6 Sanctions for Unauthorized Actions” of the CPS.

5.3.7 Independent Contractor Requirements

Shall be defined in “5.3.7 Independent Contractor Requirements” of the CPS.

5.3.8 Documentation Supplied to Personnel

Shall be defined in “5.3.8 Documentation Supplied to Personnel” of the CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Shall be defined in “5.4.1 Types of Events Recorded” of the CPS.

5.4.2 Frequency of Processing Log

Shall be defined in “5.4.2 Frequency of Processing Log” of the CPS.

5.4.3 Retention Period for Audit Log

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

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

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

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

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

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

5.4.4 Protection of Audit Log

Shall be defined in “5.4.4 Protection of Audit Log" of the CPS.

5.4.5 Audit Log Backup Procedures

Shall be defined in “5.4.5 Audit Log Backup Procedures” of the CPS.

5.4.6 Audit Collection System (internal vs. external)

Shall be defined in “5.4.6 Audit Collection System (internal vs. external)” of the CPS.

5.4.7 Notification to Event-causing Subject

Shall be defined in “5.4.7 Notification to Event-causing Subject” of the CPS.

5.4.8 Vulnerability Assessments

Shall be defined in “5.4.8 Vulnerability Assessments” of the CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

Shall be defined in “5.5.1 Types of Records Archived” of the CPS.

5.5.2 Retention Period for Archive

The Certification Authority shall archive the records prescribed in "5.5.1 Types of Records Archived" of this CP for at least 7 years beyond the effective period of the relevant certificate.

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

5.5.3 Protection of Archive

Shall be defined in “5.5.3 Protection of Archive" of the CPS.

5.5.4 Archive Backup Procedures

Shall be defined in “5.5.4 Archive Backup Procedures” of the CPS.

5.5.5 Requirements for Time-stamping of Records

Shall be defined in “5.5.5 Requirements for Time-stamping of Records” of the CPS.

5.5.6 Archive Collection System (internal or external)

Shall be defined in “5.5.6 Archive Collection System (internal or external)” of the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Shall be defined in “5.5.7 Procedures to Obtain and Verify Archive Information” of the CPS.

5.6 Key Changeover

Shall be defined in “5.6 Key Changeover” of the CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Shall be defined in “5.7.1 Incident and Compromise Handling Procedures” of the CPS.

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

Shall be defined in “5.7.2 Computing Resources, Software, and/or Data Are Corrupted” of the CPS.

5.7.3 Entity Private Key Compromise Procedures

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

The Certification Authority revokes a subscriber's certificate based on the "4.9.3 Procedure for Revocation Request" of this CP.

5.7.4 Business Continuity Capabilities after a Disaster

Shall be defined in “5.7.4 Business Continuity Capabilities after a Disaster” of the CPS.

5.8 CA or RA Termination

Shall be defined in “5.8 CA or RA Termination” of the CPS.

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 and an OCSP server is generated based on instructions of the Certification Authority Supervisor by multiple Issuing Authority System Administrators under the control of the Issuing Authority Manager.

Upon generating the key pair of the Certification Authority, a private key cryptographic module (the "HSM") that satisfies the FIPS 140-2 Level 4 standard and other methods of secret sharing shall be used. Upon generating the key pair used in an OCSP server, the HSM that satisfies the FIPS 140-2 Level 3 standard shall be used.

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

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

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

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

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

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

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

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

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

A subscriber shall include the public key in the data for requesting the issuance of a certificate, and then deliver the same to the Certification Authority via the website provided by Cybertrust.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

Name of Certification Authority	Algorithm Type	Key Length
Cybertrust Japan SureServer CA G4	SHA2 with RSA	2048 bit (with a modulus size in bits divisible by 8)

The key signature system and key length of the certificate to be used in the OCSP server shall be as follows.

Certificate to be used in OCSP Server	Algorithm Type	Key Length
Certificate issued by Cybertrust Japan SureServer CA G4	SHA2 with RSA	2048 bit (with a modulus size in bits divisible by 8)

The key signature system and key length of the subscriber's certificate shall be as follows.

subscriber's certificate;	Algorithm Type	Key Length
Certificate issued by Cybertrust Japan SureServer CA G4	SHA2 with RSA	2048 bit (with a modulus size in bits divisible by 8)

6.1.6 Public Key Parameters Generation and Quality Checking

All CA keys are generated on FIPS 140-2 qualified hardware and meets the requirements of FIPS 186-2, which ensures the proper parameters and their quality for Public Keys.

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

The key usage of certificates of the Certification Authority shall be Certificate Signing, CRL Signing. The key usage of a subscriber's certificate shall be Digital Signature, Key Encipherment.

The key usage of a certificate for use in the Certification Authority's OCSP server shall be Digital Signature.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

The key pair used in an OCSP server is controlled based on the HSM that satisfies the FIPS 140-2 Level 3 standard. The OCSP server is controlled by the Issuing Authority.

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

Shall be defined in “6.2.2 Private Key (n out of m) Multi-person Control” of the CPS.

6.2.3 Private Key Escrow

The Certification Authority does not escrow the private key of the Certification Authority and of subscribers.

6.2.4 Private Key Backup

Shall be defined in “6.2.4 Private Key Backup” of the CPS.

6.2.5 Private Key Archival

Shall be defined in “6.2.5 Private Key Archival” of the CPS.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Shall be defined in “6.2.6 Private Key Transfer into or from a Cryptographic Module” of the CPS.

6.2.7 Private Key Storage on Cryptographic Module

The private key used by the Certification Authority shall be stored in the HSM that satisfies the standards of FIPS 140-2 Level 4.

The private key used by the OCSP server shall be stored in the HSM that satisfies the standards of FIPS 140-2 Level 3.

6.2.8 Method of Activating Private Key

Shall be defined in “6.2.8 Method of Activating Private Key” of the CPS.

6.2.9 Method of Deactivating Private Key

Shall be defined in “6.2.9 Method of Deactivating Private Key” of the CPS.

6.2.10 Method of Destroying Private Key

Shall be defined in “6.2.10 Method of Destroying Private Key” of the CPS.

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity periods of certificates of the Certification Authority shall be as per the following table.

Type	Private Key	Certificate
Certificates of the Certification Authority	Not specified	No more than 120 months
Certificate to be used in OCSP Server	Not specified	25 months
SureServer Certificate	Not specified	397 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Shall be defined in “6.4.1 Activation Data Generation and Installation” of the CPS.

6.4.2 Activation Data Protection

Shall be defined in “6.4.2 Activation Data Protection" of the CPS.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Shall be defined in “6.5.1 Specific Computer Security Technical Requirements" of the CPS.

6.5.2 Computer Security Rating

Shall be defined in “6.5.2 Computer Security Rating" of the CPS.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Shall be defined in “6.6.1 System Development Controls" of the CPS.

6.6.2 Security Management Controls

Shall be defined in “6.6.2 Security Management Controls" of the CPS.

6.6.3 Life Cycle Security Controls

Shall be defined in “6.6.3 Life Cycle Security Controls" of the CPS.

6.7 Network Security Controls

Shall be defined in “6.7 Network Security Controls" of the CPS.

6.8 Time-stamping

Shall be defined in “6.8 Time-stamping” of the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

This Certification Authority issues X.509 version 3 Certificates.

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

7.1.2 Certificate Extensions

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

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

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

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

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

7.1.3 Algorithm Object Identifiers

The Certification Authority signs certificates using SHA256 with RSA in accordance with BR, Mozilla Root Store Policy, and the Relevant Requirements.

This Certification Authority issues any subscriber certificates using the SHA-1 hash algorithm.

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

7.1.4 Name Forms

The Certification Authority uses distinguished names that are composed of standard attribute types, such as those identified in RFC 5280. The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuer CA to support name chaining as specified in section 4.1.2.4 of RFC 5280. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. The Certification Authority shall restrict OU fields from containing Subscriber information that is not verified in accordance with Section 3. The OU field also must not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. The subjectAltName extension must be present and contain at least one FQDN or iPAddress, and those included in the certificate shall be validated based on section 3.2.2.4 of this CP.

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

7.1.5 Name Constraints

This Certification Authority may include name constraint in the Name Constraints field if needed.

7.1.6 Certificate Policy Object Identifier

When the Certification Authority issues a certificate containing one or more than one of the following policy identifiers, it asserts that the certificate is managed in accordance with the policy that is identified herein.

Name of the Policy	OID
Cybertrust Japan SureServer Certificate Policy (This CP)	1.2.392.200081.1.22.1
CA/Browser Forum BR OV Certificate Policy	2.23.140.1.2.2

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

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

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

i. keyCompromise (1),
ii. cACompromise (2),
iii. affiliationChanged (3),
iv. superseded (4),
v. cessationOfOperation (5),

7.2.1 Version Number(s)

The Certification Authority issues version 2 CRLs that conform to RFC 5280.

Matters regarding the CRL issued by this Certification Authority are set forth in Appendix B of this CP.

7.2.2 CRL and CRL Entry Extensions

Matters regarding the CRL issued by this Certification Authority are set forth in Appendix B of this CP.

7.3 OCSP Profile

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

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

7.3.1 Version Number(s)

Matters regarding the certificates used in the OCSP server are set forth in Appendix B.

7.3.2 OCSP Extensions

Matters regarding the certificates used in the OCSP server are set forth in Appendix B.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The Certification Authority shall verify the WebTrust Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security once a year, or perform a visiting audit at the times deemed necessary by CTJ PA.

8.2 Identity/Qualifications of Assessor

A qualified outside auditor shall verify the WebTrust Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security.

8.3 Assessor's Relationship to Assessed Entity

Shall be defined in "8.3 Assessor's Relationship to Assessed Entity" of the CPS.

8.4 Topics Covered by Assessment

The scope of audit shall be the scope set forth in the programs of the WebTrust Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security.

8.5 Actions Taken as a Result of Deficiency

Shall be defined in "8.5 Actions Taken as a Result of Deficiency" of the CPS.

8.6 Communication of Results

Validation results of the Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network are published according to the provisions of the respective guidelines.

The results of each audit are reported to the CTJPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of Cybertrust's WebTrust for CAs audit reports can be found at: https://www.cybertrust.co.jp/. On an annual basis and within three months of completion, Cybertrust submits copies of relevant audit compliance reports to SECOM Trust Systems, various parties, such as Mozilla and etc.

8.7 Self Audit

On at least a quarterly basis, the Certification Authority performs regular internal audits against a randomly selected sample of at least three percent of Certificates since the last internal audit.

9. Other Business and Legal Matters

9.1 Fees

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

Moreover, if the Certification Authority is requested by a subscriber to reissue a certificate based on the following reasons, the Certification Authority shall reissue a certificate that is valid for the remaining period, free of charge so as long as such request is made within thirty (30) days after the issuance of the original certificate in principle. The original certificate shall basically be revoked.:

i. the key pair generated during the application was unintentionally erased or damaged;
ii. the original certificate cannot be used due to server replacement;
iii. the password required for downloading a certificate based on “4.4.1 Conduct Constituting Certificate Acceptance" of this CP is lost; or
iv. the Certification Authority otherwise deems it appropriate.

9.2 Financial Responsibility

Shall be defined in “9.2 Financial Responsibility” of the CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Shall be defined in “9.3.1 Scope of Confidential Information” of the CPS.

9.3.2 Information not within the Scope of Confidential Information

Shall be defined in “9.3.2 Information not within the Scope of Confidential Information” of the CPS.

9.3.3 Responsibility to Protect Confidential Information

Shall be defined in “9.3.3 Responsibility to Protect Confidential Information" of the CPS.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Shall be defined in “9.4.1 Privacy Plan" of the CPS.

9.4.2 Information Treated as Private

Shall be defined in “9.4.2 Information Treated as Private" of the CPS.

9.4.3 Information not Deemed Private

Shall be defined in “9.4.3 Information not Deemed Private" of the CPS.

9.4.4 Responsibility to Protect Private Information

Shall be defined in “9.4.4 Responsibility to Protect Private Information" of the CPS.

9.4.5 Notice and Consent to Use Private Information

Shall be defined in “9.4.5 Notice and Consent to Use Private Information" of the CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Shall be defined in “9.4.6 Disclosure Pursuant to Judicial or Administrative Process" of the CPS.

9.4.7 Other Information Disclosure Circumstances

Shall be defined in “9.4.7 Other Information Disclosure Circumstances” of the CPS.

9.5 Intellectual Property Rights

Shall be defined in “9.5 Intellectual Property Rights” of the CPS.

9.6 Representations and Warranties

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

9.6.1 CA Representations and Warranties

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

i. safely control the Certification Authority private key;
ii. perform accurate certificate issuance and revocation based on the application from the Registration Authority;
iii. provide revocation information by issuing and publishing CRL and by using the OCSP server;
iv. monitor and operate the system; and
v. maintain and control the repositories.

9.6.2 RA Representations and Warranties

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

i. perform screening of subscribers based on this CP;
ii. properly handle certificate issuance applications and revocation requests to the Issuing Authority; and
iii. accept inquiries ("1.5.2 Contact Person" of this CP).

9.6.3 Subscriber Representations and Warranties

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

i. provide correct and accurate information upon applying for the issuance of a certificate;
ii. strictly manage the private key and password to ensure the confidentiality and integrity thereof;
iii. refrain from installing a certificate in a server and using the certificate until the accuracy of the information included in the certificate is confirmed;
iv. install a certificate only in a server that is accessible by the subjectAltName included in the certificate, and use the certificate according to the applicable law and regulations and the Subscriber Agreement;
v. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber’s Private Key associated with the Public Key included in the Certificate;
vi. promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise;
vii. respond to the Certification Authority's instruction within a specified period upon the occurrence of an event set forth in “4.9.1.1 Reason of Revocation" of this CP;
viii. acknowledge and accept thar the Certification Authority is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the Certification Authority’s CP, CPS, or relevant requirements set forth by CA/Browser Forum

ix. refrain from submitting or using the certificate with the OU attribute listed in the certificate when including the name, DBA, product name, trademark, address, location, or other text that refers to a specific natural person or Legal entity unless the Certification Authority verifies that specified information indicates the Subscriber. This field MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable;
x. comply with the usage of the certificate (“1.4.1 Appropriate Certificate Uses" of this CP);
xi. refrain from using the certificate in websites that are contrary to public order and morals;
xii. refrain from using an expired certificate or a revoked certificate; and
xiii. observe applicable laws and regulations.

9.6.4 Relying Party Representations and Warranties

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

i. confirm that the certificates are being used for the usage set forth in "1.4.1 Appropriate Certificate Uses" of this CP;
ii. confirm the effective period and entries of certificates issued by the Certification Authority;
iii. verify the digital signature and verify the issuer of the certificate;
iv. confirm whether the certificate has been revoked based on CRL or OCSP; and
v. bear legal liability for situations arising from the default of obligations prescribed in this paragraph.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

The Certification Authority shall not be liable for any default based on this CP regarding damages excluding direct damages arising in relation to the warranties set forth in "9.6.1 CA Representations and Warranties" and "9.6.2 RA Representations and Warranties" of this CP.

The Certification Authority shall not be liable in any way for the consequences resulting from a relying party trusting the certificates of the Certification Authority and subscribers based on its 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 CA representations and Warranties" and "9.6.2 RA representations and Warranties" of this CP:

i. any damage that arises regardless of the Certification Authority of Cybertrust observing this CP, the CPS, the Guidelines specified in “1.1 Overview" of this CP, 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 subscribers or relying parties neglecting to perform their respective obligations prescribed in “9.6 Representations and Warranties" of this CP;
iv. damage that arises as a result of the key pair of the certificate issued by the Certification Authority being divulged due to acts of a third party other than Cybertrust;
v. damage that arises as a result of the certificate infringing upon the copyright, trade secret or any other intellectual property right of the subscriber, a relying party or a third party; or
vi. damage caused by improvement in the encryption algorithm decoding technology, based on hardware or software, exceeding current expectations.

The total amount of damages to be borne by Cybertrust against subscribers and relying parties or other third parties with regard to any and all damages arising in relation to the application, approval, trust or any other use of the certificates of the Certification Authority shall 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 CP, the CPS, the Subscriber Agreement, or the Related Rules, the Certification Authority shall not be liable for any data loss, indirect damages including lost profits, consequential damages and punitive damages to the extent permitted under the governing law set forth in "9.14 Governing Law" of the CPS.

9.9 Indemnities

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

i. unauthorized use, falsification, or misrepresentation during the use of a certificate;
ii. breach of this CP, theCPS, or the Subscriber Agreement; or
iii. neglect by a subscriber to preserve the private key.

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

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

The Certification Authority shall annually review this CP based on instructions from CTJ PA. This CP may be amended if needed. CTJ PA shall approve the amendment after obtaining the evaluation of the Certification Authority Staff or the evaluation of outside professionals such as attorneys or other experts.

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under Which OID Must Be Changed

CTJPA is responsible to decide if the OID updates are required correspondingly to this CP change.

9.13 Dispute Resolution Provisions

Shall be defined in “9.13 Dispute Resolution Provisions” of the CPS.

9.14 Governing Law

Shall be defined in “9.14 Governing Law” of the CPS.

9.15 Compliance with Applicable Law

Shall be defined in “9.15 Compliance with Applicable Law” of the CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (attorneys’ fees and waiver of rights)

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

9.16.5 Force Majeure

In the event the performance of a part or all of the obligations under this CP or the CPS is delayed because of 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 CP or the CPS during the delay period, and shall not be liable in any way against a subscriber or a third party that trusted or used a certificate.

9.17 Other Provisions

Not applicable.

Appendix A: List of Definitions

Term	Definition
Archive	As used herein, the term "archive" refers to the process of storing expired certificates for a predetermined period.
Cryptographic Module	Software, hardware, or a device configured from the combination of such software and hardware that is used for ensuring security in the generation, storage and use of private keys.
Suspension	Measure for temporarily invalidating a certificate during the effective period of that certificate.
Key Length	A bit number that represents the key length which is also a factor in deciding the cryptographic strength.
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 the other key.
Activation	To cause a system or device to be usable. Activation requires activation data, and specifically includes a PIN and pass phrase.
Subscriber Agreement	An agreement to be accepted by a subscriber to apply for and use a certificate. This CP constitutes a part of the Subscriber Agreement.
Compromise	A state where the confidentiality or integrity 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.).
Independent Contractor	A person who meets all the following conditions. ・A person who is 20 years old or older and runs a business as an individual ・A person who notified the country or municipality of the start of a business and actually runs the business A person who indicates the shop name of the business on the business name registration, business commencement form, and tax declaration
Revocation	Measure for invalidating a certificate even during the effective period of that certificate.
Certificate Revocation List	Abbreviated as "CRL" in this CP. CRL is a list of revoked certificates. The Certification Authority publishes CRL so that the relying parties can verify the validity of certificates.
Certification Operations	Series of operations that are performed during the life cycle controls of certificates. Including, but not limited to, operations of accepting issuance/revocation requests, 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 third parties other than a subscriber.
Main Site	A facility equipped with assets of the Certification Authorities required for certificate issuance and revocation.
Escrow	As used herein, the term "deposit" refers to the processing of registering and storing a private key or a public key at a third party.
Repository	A website or system for posting public information such as this CP and CRL.
Root CA	A certification authority above the Certification Authority. It issues certificates of the Certification Authority.
ACME	Abbreviation for "Automated Certificate Management Environment" and it is a standard protocol for automate the processes of domain names verification, installation, and management for X.509 certificates.
ALPN	Abbreviation for "Application-Layer Protocol Negotiation" and it is an extended function of TLS.
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (BR)	Requirements for issuing publicly-trusted certificates which were formulated by the CA/Browser Forum.
CA/Browser Forum	Organization that consists of the Certification Authorities that issue publicly-trusted certificates for SSL/TLS communications and the companies that develop applications such as browsers. It creates standards about certificates. The website of the organization is https://cabforum.org/.
Certificate Transparency	A scheme standardized in RFC6962 for promptly discovering and detecting fraudulent certificates.
DBA/Tradename	Indicates a common name, trade name, shop name, trademark, etc. other than the legal name of an organization.
Distinguished Name	An identifier set forth in the X.500 recommendation formulated by ITU-T. Configured from attribute information such as a common name, organization name, organizational unit name, and country name.
DNS CAA Email Contact	The email address defined in APPENDIX A.1.1 of BR.
DNS CAA Phone Contact	The phone number defined in APPENDIX A.1.2 of BR.
DNS Certification Authority Authorization Resource Record (CAA Record)	One of the DNS records defined in RFC8659 which aims to clarify the certification authority to issue the server certificate to a domain name and prevent the issuance of unintended certificates.
DNS TXT Record Email Contact	The email address defined in APPENDIX A.2.1 of BR.
DNS TXT Record Phone Contact	The phone number defined in APPENDIX A.2.2 of BR.
FIPS 140-2	FIPS (Federal Information Processing Standards Publication 140) is a U.S. federal standard that prescribes the specifications of security requirements in a cryptographic module, and the latest version of this standard is 2. With this standard, the security requirements are classified as the levels of 1 (lowest) to 4 (highest).

Fully-Qualified Domain Name (FQDN)	A domain name to which a sub domain name and a host name are added and is included in a certificate.
IETF PKIX Working Group	Internet Engineering Task Force (IETF) is an organization that standardizes technologies used for the Internet, and the PKIX Working Group of IETF set forth RFC3647.
IP Address	32-bit or 128-bit label that is assigned to a device that uses the Internet Protocol for communications.
IP Address Contact	A person or organization authorized to control the method of using one or more IP addresses that is registered in an IP address registration authority.
IP Address Registration Authority	Internet Assigned Numbers Authority (IANA) or Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
ITU-T	Telecommunications Standardization Sector of the International Telecommunication Union.
Name Constraints	Registration of the Key Usage and Name Constraint extensions in a certificate of a certification authority to restrict the issue of a certificate.
OCSP	Abbreviation of "Online Certificate Status Protocol", and is a communication protocol for providing certificate revocation information. The Certification Authority is operating an OCSP server, in addition to publicly disclosing CRL, so that a relying party can verify the validity of a certificate.
Punycode	Punycode is a method, defined in RFC 3492, designed to encode an Internationalized Domain Names (IDN). The value transformed its Unicode string into an ASCII characters with ACE prefix "xn---" added in accordance with Punycode encoding method shall be called "A-label".
RFC7231	The document named "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content" defining semantics of HTTP/1.1 message which is set forth by the IETF PKIX Working Group.
RFC7538	The document named "The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)" defining the additional Hypertext Transfer Protocol (HTTP) status code 308 (Permanent Redirect) which is set forth by the IETF PKIX Working Group.
RSA	Public key cryptography developed by Rivest, Shamir, and Adelman.
SHA1/SHA2	A hash function used in digital signatures, etc. A hash function is used for reducing data into a given length based on mathematical operations, and makes it infeasible to calculate the same output value from two different input values. It is also infeasible to inverse the input value from the output value.
SSL/TLS	A protocol for encrypting and sending/receiving information on the Internet which was developed by Netscape Communications. TLS is an improvement of SSL 3.0.
WebTrust 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 Principles and Criteria for Certification Authorities – SSL Baseline with Network Security	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 Certificate

Cybertrust Japan SureServer CA G4

Intermediate CA Certificate (Validity Period：September 27, 2019 to May 29, 2029)

(Basic Certificate Fields)

version		**value**
Version	Version of the encoded certificate type:INTEGER	 2 (Ver.3)
serialNumber		**value**
CertificateSerialNumber	Serial number of certificate type:INTEGER	 6405698833811812014 54 (0x22b9b1630cecb43c2e)
signature		**value**
AlgorithmIdentifier algorithm parameters	The identifier for the cryptographic algorithm used by the CA to sign this certificate (Public key cryptosystem and hash) Object ID for the cryptographic algorithm type:OID Parameters of cryptographic algorithm type:NULL	 1.2.840.113549.1.1.11 (SHA-256) NULL
issuer		**value**
countryName type value organizationName type value organaizationalUnitName type value	Country name attribute of certificate issuer Object ID for the country name type:OID Value of country name type:PrintableString Organization name attribute of certificate issuer Object ID for organization name type:OID Value of organization name type:PrintableString Organizational unit name attribute of certificate issuer Object ID for organizational unit name type:OID Value of organizational unit name type:PrintableString	 2.5.4.6 JP 2.5.4.10 SECOM Trust Systems CO., LTD. 2.5.4.11 Security Communication RootCA2
validity		**value**
Validity notBefore notAfter 	Validity period of the certificate The date on which the certificate validity period begins type:UTCTime The date on which the certificate validity period ends type:UTCTime	 190927015423Z (September 27, 2019 10:54:23 JST) 290529050039Z (May 29, 2029 14:00:39 JST)
subject		**value**
countryName type value organizationName type value commonName type value	Country name attribute of certificate subject Object ID for the country name type:OID Value of country name type:PrintableString Organization name attribute of certificate subject Object ID for organization name type:OID Value of organization name type:PrintableString Common name attribute of certificate subject Object ID for common name type:OID Value of common name	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3

	type:PrintableString	Cybertrust Japan SureServer CA G4
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject’s public key information	
AlgorithmIdentifier	The identifier for cryptographic algorithm (public key cryptosystem and hash)	
algorithm	Object ID for the cryptographic algorithm type:OID	1.2.840.113549.1.1.1 (RSA encryption)
parameters	Parameters of cryptographic algorithm type:NULL	NULL
subjectPublicKey	Value of public key type:BIT STRING	*Public key of 2048 bit length

(Certificate Extensions)

subjectKeyIdentifier (extnId :== 2 5 29 14, critical :== FALSE)		**value**
SubjectKeyIdentifier	Information of Subject Key Identifier	
KeyIdentifier	The identifier for public key type:OCTET STRING	62:A7:D2:DA:DE:85:B6:92:F1:85:BC:F6:E8:95:9D:75:A0:FA:4E:1F
certificatePolicies (extnId :== 2 5 29 32, critical :== FALSE)		**value**
PolicyInformation	Information of the Policy	
policyIdentifier	Object ID for the Policy type:OID	1.2.392.200091.100.901.4
policyQualifiers	Information of the policy qualifiers	
PolicyQualifierID	Classification of the policy qualifiers type:OID	1.3.6.1.5.5.7.2.1 (CPSuri)
Qualifier	URI of CPS is published type:IA5String	https://repository.secomtrust.net/SC-Root2/
cRLDistributionPoints (extnId :== 2 5 29 31, critical :== FALSE)		**value**
CRLDistributionPoints	CRL Distribution Point	
DistributionPoint	CRL Distribution Point	
uniformResourceIdentifier	URI of CRL Distribution Point type:IA5String	http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1, critical :== FALSE)		**value**
AuthorityInfoAccess	Authority Information Access	
AccessDescription	Online Certificate Status Protocol	
accessMethod	Access method type:OID	1.3.6.1.5.5.7.48.1 (ocsp)
accessLocation	Access location type:IA5String	http://scrootca2.ocsp.secomtrust.net
AccessDescription	Issuer of the Authority	
accessMethod	Access method type:OID	1.3.6.1.5.5.7.48.2 (calssuers)
accessLocation	Access location type:IA5String	http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer
authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier	Authority Key Identifier	
KeyIdentifier	The identifier for public key type:OCTET STRING	0A:85:A9:77:65:05:98:7C:40:81:F8:0F:97:2C:38:F1:0A:EC:3C:CF
keyUsage (extnId :== 2 5 29 15, critical :== TRUE)		**value**
KeyUsage	Key Usage type:BIT STRING	00000110 (0x06) (keyCertSign, cRLSign)
extKeyUsage (extnId :== 2 5 29 37, critical :== FALSE)		**value**
ExtKeyUsage	Extended Key Usage	
KeyPurposeId	The purpose of the key contained in the certificate type:OID	1.3.6.1.5.5.7.3.1 (serverAuth) 1.3.6.1.5.5.7.3.2 (clientAuth)
basicConstraints (extnId :== 2 5 29 19, critical :== TRUE)		**value**
BasicConstraints	Basic Constraints	
cA	The flag to determine whether the supplied certificate is associated with a CA or an end entity type:BOOLEAN	TRUE
pathLenConstraint	Path length constraint type:INTEGER	0

SureServer [SHA-2] Certificate

(Basic Certificate Fields)

version		**value**
Version	Version of the encoded certificate type:INTEGER	2 (Ver.3)
serialNumber		**value**
CertificateSerialNumber	Serial number of certificate type:INTEGER	*Serial number of certificate (unique positive integer)
signature		**value**
AlgorithmIdentifier	The identifier for the cryptographic algorithm used by the CA to sign this certificate (Public key cryptosystem and hash)	
algorithm	Object ID for the cryptographic algorithm type:OID	1.2.840.113549.1.1.11 (SHA-256)
parameters	Parameters of cryptographic algorithm type:NULL	NULL
issuer		**value**
countryName	Country name attribute of certificate issuer	
type	Object ID for the country name type:OID	2.5.4.6
value	Value of country name type:PrintableString	JP
organizationName	Organization name attribute of certificate issuer	
type	Object ID for organization name type:OID	2.5.4.10
value	Value of organization name type:PrintableString	Cybertrust Japan Co., Ltd.
commonName	Common name attribute of certificate issuer	
type	Object ID for common name type:OID	2.5.4.3
value	Value of common name type:PrintableString	Cybertrust Japan SureServer CA G4
validity		**value**
Validity	Validity period of certificate	
notBefore	The date on which the certificate validity period begins type:UTCTime	*The date on which the certificate validity period begins
notAfter	The date on which the certificate validity period ends type:UTCTime	*The date on which the certificate validity period ends
subject		**value**
countryName	Country name attribute of certificate subject	
type	Object ID for the country name type:OID	2.5.4.6
value	Value of country name type:PrintableString	*Country name attribute of certificate subject
stateOrProvinceName	State or Province name attribute of certificate subject	
type	Object ID for the state or province name type:OID	2.5.4.8
value	Value of state or province name type:PrintableString / UTF8String	*State or province name attribute of certificate subject
localityName	Locality name attribute of certificate subject	
type	Object ID for the locality name type:OID	2.5.4.7
value	Value of locality name type:PrintableString / UTF8String	*Locality name attribute of certificate subject
organizationName	Organization name attribute of certificate subject	
type	Object ID for organization name type:OID	2.5.4.10
value	Value of organization name type:PrintableString / UTF8String	*Organization name attribute of

		certificate subject
organizationalUnitName	Organizational unit name attribute of certificate subject	*When necessary
type	Object ID for the organizational unit name type:OID	2.5.4.11
value	Value of organizational unit name type:PrintableString / UTF8String	*Organization unit name attribute of certificate subject
commonName	Common name attribute of certificate subject	
type	Object ID for common name type:OID	2.5.4.3
value	Value of common name type:PrintableString	*FQDN of the SSL/TLS server
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject's public key information	
AlgorithmIdentifier	The identifier for cryptographic algorithm (public key cryptosystem and hash)	
algorithm	Object ID for the cryptographic algorithm type:OID	1.2.840.113549.1.1.1 (RSA encryption)
parameters	Parameters of cryptographic algorithm type:NULL	NULL
subjectPublicKey	Value of public key type:BIT STRING	*The key length depends on application *The key length must be at least 2048 bit

(Certificate Extensions)

basicConstraints (extnId :== 2 5 29 19, critical :== TRUE)		**value**
BasicConstraints	Basic Constraints	
cA	The flag to determine whether the supplied certificate is associated with a CA or an end entity type:BOOLEAN	FALSE
certificatePolicies (extnId :== 2 5 29 32, critical :== FALSE)		**value**
PolicyInformation	Information of the Policy	
policyIdentifier	Object ID for the Policy type:OID	1.2.392.200081.1.23.1
policyQualifiers	Information of the policy qualifiers	
PolicyQualifierID	Classification of the policy qualifiers type:OID	1.3.6.1.5.5.7.2.1 (CPSuri)
Qualifier	URI of CPS is published type:IA5String	https://www.cybertrust.ne.jp/ssl/repository/index.html
PolicyInformation	Information of the Policy	
policyIdentifier	Object ID for the Policy type:OID	2.23.140.1.2.2 (organization-validated)
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1, critical :== FALSE)		**value**
Authority Information Access	Authority Information Access	
AccessDescription	Online Certificate Status Protocol	
accessMethod	Access method type:OID	1.3.6.1.5.5.7.48.1 (ocsp)
accessLocation	Access location type:IA5String	http://ssocsp.cybertrust.ne.jp/OcspServer
AccessDescription	Issuer of the Authority	
accessMethod	Access method type:OID	1.3.6.1.5.5.7.48.2 (caIssuers)
accessLocation	Access location type:IA5String	http://crl.cybertrust.ne.jp/SureServer/ovcag4/ovcag4.crt
subjectAltName (extnId :== 2 5 29 17, critical :== FALSE)		**value**
SubjectAltName	Subject Alternative Name	
dNSName	DNS Name type:IA5String	*FQDN or IP address of the SSL/TLS server
keyUsage (extnId :== 2 5 29 15, critical :==TRUE)		**value**
KeyUsage	Key Usage type:BIT STRING	10100000 (0xA0) (digitalSignature, keyEncipherment)
extKeyUsage (extnId :== 2 5 29 37, critical :== FALSE)		**value**
ExtKeyUsage	Extended Key Usage	
KeyPurposeId	The purpose of the key contained in the certificate type:OID	1.3.6.1.5.5.7.3.1 (serverAuth)

		1.3.6.1.5.5.7.3.2 (clientAuth)
authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier KeyIdentifier	Authority Key Identifier The identifier for public key type:OCTET STRING	62:A7:D2:DA:DE:85:B6:92:F1:85:BC:F6:E8:95:9D:75:A0:FA:4E:1F
cRLDistributionPoints (extnId :== 2 5 29 31, critical :== FALSE)		**value**
CRLDistributionPoints DistributionPoint uniformResourceIdentifier	CRL Distribution Point CRL Distribution Point URI of CRL Distribution Point type:IA5String	http://crl.cybertrust.ne.jp/SureServer/ovcag4/cdp.crl
subjectKeyIdentifier (extnId :== 2 5 2 14, critical :== FALSE)		**value**
SubjectKeyIdentifier KeyIdentifier	Subject Key Identifier The identifier for public key type:OCTET STRING	*Hash value of the BIT STRING subjectPublicKey
(extnId :== 1 3 6 1 4 1 11129 2 4 2, critical :== FALSE) (*1)		**value**
1.3.6.1.4.1.11129.2.4.2	Object ID for Certificate Transparency type:OCTET STRING	＊Signed CertificateTimestamp List

OCSP Server Certificate

(Basic Certificate Fields)

version		**value**
Version	Version of the encoded certificate type:INTEGER	2 (Ver.3)
serialNumber		**value**
CertificateSerialNumber	Serial number of certificate type:INTEGER	*Serial number of certificate (unique positive integer)
signature		**value**
AlgorithmIdentifier	The identifier for the cryptographic algorithm used by the CA to sign this certificate (public key cryptosystem and hash)	
algorithm	Object ID for the cryptographic algorithm type:OID	1.2.840.113549.1.1.11 (SHA-256)
parameters	Parameters of cryptographic algorithm type:NULL	NULL
issuer		**value**
countryName	Country-name attribute of certificate issuer	
type	Object ID for the country name type:OID	2.5.4.6
value	Value of country name type:PrintableString	JP
organizationName	Organization name attribute of certificate issuer	
type	Object ID for organization name type:OID	2.5.4.10
value	Value of organization name type:PrintableString	Cybertrust Japan Co., Ltd.
commonName	Common name attribute of certificate issuer	
type	Object ID for common name type:OID	2.5.4.3
value	Value of common name type:PrintableString	Cybertrust Japan SureServer CA G4
validity		**value**
Validity	Validity period of certificate	
notBefore	The date on which the certificate validity period begins type:UTCTime	*The date on which the certificate validity period begins
notAfter	The date on which the certificate validity period ends type:UTCTime	*The date on which the certificate validity period ends
subject		**value**
countryName	Country name attribute of certificate subject	
type	Object ID for the country name type:OID	2.5.4.6
value	Value of country name type:PrintableString	JP
organizationName	Organization name attribute of certificate subject	
type	Object ID for organization name type:OID	2.5.4.10
value	Value of organization name type:PrintableString	Cybertrust Japan Co., Ltd.
commonName	Common name attribute of certificate subject	
type	Object ID for common name type:OID	2.5.4.3
value	Value of common name type:PrintableString	Cybertrust Japan SureServer CA G4 OCSP Responder
subjectPublicKeyInfo		**value**
SubjectPublicKeyInfo	Subject’s public key information	
AlgorithmIdentifier	The identifier for cryptographic algorithm (public key cryptosystem and hash)	
algorithm	Object ID for the cryptographic algorithm type:OID	1.2.840.113549.1.1.1 (RSA encryption)
parameters	Parameters of cryptographic algorithm	

	type:NULL	NULL
subjectPublicKey	Value of public key type:BIT STRING	*Public key of 2048 bit length

(Certificate Extensions)

basicConstraints (extnId :== 2 5 29 19, critical :== FALSE)		**value**
BasicConstraints cA	Basic Constraints The flag to determine whether the supplied certificate is associated with a CA or an end entity type:BOOLEAN	FALSE
authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier KeyIdentifier	Authority Key Identifier The identifier for public key type:OCTET STRING	62:A7:D2:DA:DE:85:B6:92:F1:85:BC:F6:E8:95:9D:75:A0:FA:4E:1F
subjectKeyIdentifier (extnId :== 2 5 2 14, critical :== FALSE)		**value**
SubjectKeyIdentifier KeyIdentifier	Subject Key Identifier The identifier for public key type:OCTET STRING	*Hash value of the BIT STRING subjectPublicKey
keyUsage (extnId :== 2 5 29 15, critical :== TRUE)		**value**
KeyUsage	Key Usage type:BIT STRING	10000000 (0x80) (digitalSignature)
extKeyUsage (extnId :== 2 5 29 37, critical :== FALSE)		**value**
ExtKeyUsage KeyPurposeId	Extended Key Usage The purpose of the key contained in the certificate type:OID	1.3.6.1.5.5.7.3.9 (OCSPSigning)
OCSP No Check (extnId :== 1 3 6 1 5 5 7 48 1 5, critical :== FALSE)		**value**
OCSP No Check OCSP No Check	Revocation checking of signer certificates Do not check revocation	NULL

CRL

(CRL Fields)

version		**value**
Version	Version of the CRL(Revocation list) type:INTEGER	1 (Ver.2)
signature		**value**
AlgorithmIdentifier	The identifier for the cryptographic algorithm used by the CRL issuer to sign the CertificateList (public key cryptosystem and hash)	*Use of SHA-1 algorithm for CRLs are only used in compliance with BR, Mozilla Root Store Policy or the relevant requirements.
algorithm	Object ID for the cryptographic algorithm type:OID	1.2.840.113549.1.1.11 (SHA-256)
parameters	Parameters of cryptographic algorithm type:NULL	NULL
issuer		**value**
countryName	Country name attribute of CRL issuer	
type	Object ID for the country name type:OID	2.5.4.6
value	Value of country name type:PrintableString	JP
organizationName	Organization name attribute of CRL issuer	
type	Object ID for organization name type:OID	2.5.4.10
value	Value of organization name type:PrintableString	Cybertrust Japan Co., Ltd.
commonName	Common name attribute of CRL issuer	
type	Object ID for common name type:OID	2.5.4.3
value	Value of common name type:PrintableString	Cybertrust Japan SureServer CA G4
thisUpdate		**value**
thisUpdate	The issue date of this CRL type:UTCTime	*The issue date of this CRL
nextUpdate		**value**
nextUpdate	The date by which the next CRL is issued type:UTCTime	*The date by which the next CRL is issued

(CRL Extensions)

authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**value**
AuthorityKeyIdentifier	Authority Key Identifier	
KeyIdentifier	The identifier for public key type:OCTET STRING	62:A7:D2:DA:DE:85:B6:92:F1:85:BC:F6:E8:95:9D:75:A0:FA:4E:1F
cRLNumber (extnId :== 2 5 29 20, critical :== FALSE)		**value**
cRLNumber	CRL Number type:INTEGER	*Serial number of CRL
issuingDistributionPoint (extnId :== 2 5 29 28, critical :== FALSE)		**value**
issuingDistributionPoint	CRL issuing distribution point	
distributionPoint	CRL Distribution Point	
uniformResourceIdentifier	URI of CRL Distribution Point type:IA5String	http://crl.cybertrust.ne.jp/SureServer/ovcag4/cdp.crl
onlyContainsUserCerts	The flag to indicate that CRL contains only for user certs. type:BOOLEAN	TRUE
onlyContainsCACerts	The flag to indicate that CRL contains only for CA certs. type:BOOLEAN	FALSE
indirectCRL	The flag to indicate that CRL is indirect CRL. type:BOOLEAN	FALSE

(CRL Entry)

revokedCertificates		**value**
CertificateSerialNumber	Serial number of revoked certificate type:INTEGER	*Serial number of revoked certificate
revocationDate	The date on which the revocation occurred	

	type:UTCTime	*The date on which the revocation occurred

(CRL Entry Extensions)

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