Cybertrust Device ID

Certification Practice Statement

Version 3.6

Cybertrust Japan Co., Ltd.

July 28, 2023

Revision History

Version	Date	Reason for Revision
1.0	June 29, 2009	▪ First Version
1.1	August 17, 2009	▪ Correction of typographical errors
1.2	December 1, 2009	▪ Change (abbreviation) of designated character string in consideration of the 64-byte limitation of the Organization Unit in the certificate specifically, the Organization Unit Name has been changed from "Cybertrust DeviceiD RA operated by <<Name of Customer's Company + Corporation identifier>>" to "RA operated by <<Name of Customer's Company + Corporation identifier>>"
1.3	May 12, 2010	▪ Addition of description related to the Network Equipment Dedicated Server Certificate
1.4	December 1, 2010	▪ Unification of descriptions related to certificate issue targets as follows: *Devices approved by the Subscriber Management Organization *Network Equipment being used or managed by the subscriber ▪ Revision of description related to the appointment criteria of the Registration Authority Operator Supervisor ▪ Revision of description related to the corrective measures to be taken by the Registration Authority in response to the audit results ▪ Correction of typographical errors
1.5	April 28, 2011	▪ Addition of description related to the configuration profile signature certificate ▪ Unification/revision of certain indications
1.6	March 28, 2013	▪ Pursuant to the suspension of issuance of the configuration profile signature certificate by the Certification Authority, deletion of description related to such certificate ▪ Reflection of change in the application flow of the Network Equipment Dedicated Server Certificate ▪ Reflection of the specification change related to the invalidity date in the CRL
1.7	April 26, 2013	▪ Reflection of start of provision of the OCSP server ▪ Addition/revision of description related to the validity period of the CRL
1.8	October 22, 2013	▪ Addition/revision of description related to the 2nd generation Certification Authority ▪ Addition/revision of description related to the issue and publication of the CRL, and provision of the OCSP ▪ Correction of typographical errors
1.9	April 21, 2014	▪ Addition of description of the 2nd generation Certification Authority Cybertrust DeviceiD Public CA G2is ▪ Revision of the key renewal period of the Certification Authority, and validity period of the certificate ▪ Change of name from the Device ID Secretariat to the Device ID Support Desk ▪ Correction of typographical errors
2.0	May 14, 2015	▪ Addition of description of the 2nd generation Certification Authority Cybertrust DeviceiD Public CA G2sp ▪ Reflection of the specification change related to the invalidity date in the CRL ▪ Correction of typographical errors
2.1	July 21, 2015	▪ Addition/revision of description related to the 3rd generation Certification Authority Cybertrust DeviceiD Public CA G3k ▪ Addition of Authority Information Access to the Device ID Certificate (3rd generation Certification Authority only) ▪ Correction of typographical errors
2.2	October 15, 2015	▪ Addition of description related to 3rd generation Certification Authority Cybertrust DeviceiD Public CA G3, Cybertrust DeviceiD Public CA G3s, Cybertrust DeviceiD Public CA G3is, and Cybertrust DeviceiD Public CA G3sp

2.3	December 15, 2015	▪ Addition of description of the 2nd generation Certification Authority Cybertrust DeviceiD Public CA G2t ▪ Addition of description of the 3rd generation Certification Authority Cybertrust DeviceiD Public CA G3t
2.4	January 25, 2016	▪ Addition of userPrincipalName to the Device ID Certificate issued by Cybertrust DeviceiD Public CA G2is and Cybertrust DeviceiD Public CA G3is (option)
2.5	August 10, 2016	▪ Change of reception date of “1.5.2 Contact Person” ▪ Addition of description related to subjectAltName ▪ Revision of description related to userPrincipalName
2.6	December 15, 2016	▪ Addition of description of the 3rd generation Certification Authority Cybertrust DeviceiD Public CA G3h
2.7	December 15, 2017	▪ Change of reception date of “1.5.2 Contact Person”
2.8	February 26, 2018	▪ Addition of description of the 3rd generation Certification Authority Cybertrust DeviceiD Public CA G3isr
2.9	November 15, 2018	▪ Revision of description related to issue and publication of the CRL ▪ Unification/revision of certain indications
3.0	July 24, 2019	▪ Deletion of description regarding the 1st generation Certification Authority Cybertrust DeviceiD Public CA G1 due to expiration ▪ Update of public site URL ▪ Addition of rights and obligations of the Cybertrust Japan Policy Authority ▪ Revision of description related to authorityInfoAccess
3.1	September 11, 2019	▪ Addition of validity period and extended key usage of the Network Equipment Dedicated Server Certificate ▪ Unification/revision of certain indications
3.2	August 12, 2020	▪ Addition of cases of distributing device certificates independently ▪ Addition of description of the 3rd generation Certification Authority Cybertrust DeviceiD Education CA G3h ▪ Addition of description related to the backup site ▪ Unification/revision of certain indications
3.3	December 16, 2020	▪ Addition of description related to subjectAltName (iPAddress) of the Network Equipment Dedicated Server Certificate
3.4	December 13,2021	▪ Addition of description of the 3rd generation Certification Authority Cybertrust DeviceiD Public CA G3m ▪ Addition of the serial number of the Certificate Authority certificateand fingerprint ▪ Revision of description of the Certificate Operational Periods and Key Pair Usage Periods
3.5	January 11, 2022	▪ Addition/revision of description related to the DeviceiD Premium option ▪ Unification/revision of certain indications
3.6	July 28, 2023	▪ Additions and modifications regarding Device ID Premium Certification Authority. ▪ Revise the description related to OCSP provision in section 4.9.9 " On-line Revocation/Status Checking Availability" ▪ Revise the descriptions in "Appendix B: Certificate and Profile." ▪ Correct any typos or errors.

*Note This "**Cybertrust Device ID Certification Practice Statement**" 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 Device ID Certification Practice Statement**." Upon disclosure of the new version of "**Cybertrust Device ID Certification Practice Statement**" by Cybertrust Japan Co., Ltd., please stop referring to/using this documentation. Your understanding on above mentioned conditions is requested prior to refer to this documentation.

1. Introduction

1.1 Overview

Cybertrust Japan Co., Ltd. (“Cybertrust”) provides Cybertrust Device ID (“Service”), which is a device certificate issuance and management service.

A Subscriber Management Organization of the Service may, based on the Service, operate the Registration Authority of the Device ID Certificate, which specializes in the authentication of devices, and cause such Registration Authority to manage certificates, including the issuance and revocation of the Device ID Certificate. The Device ID Certificate is a certificate that can be used for robust authentication based on SSL/TLS, IPsec, IEEE802.1x and the like which are standard specifications in network access authentication, and a user of the Service and ensure the network safety and realize the safe utilization of information assets through integrated network access control based on the Device ID Certificate.

A Subscriber Management Organization of the Service can also receive and use a server certificate (“Network Equipment Dedicated Server Certificate”) dedicated to network equipment or server equipment (collectively, “Network Equipment”). The Network Equipment Dedicated Server Certificate is a server certificate that is essential for a Network Equipment to which the devices access using the Device ID Certificate mainly in combination with a supplicant equipped in iOS, Android and Windows OS as a standard feature.

The Device ID Certificate and the Network Equipment Dedicated Server Certificate are issued by the following Certification Authorities managed by Cybertrust. Unless otherwise prescribed herein, the term “Issuing CA（Certification Authority）” shall include the following Certification Authorities.

Name of Certification Authority	Cybertrust DeviceiD Public CA G2
Serial Number of Certification Authority Certificate	20000001
Validity Period	October 16, 2013 to November 16, 2028
Key Length	2048 bit
Signature Algorithm	SHA1withRSA
Fingerprint (SHA1)	C62805E0E1E44B7F4FE8139E07A72E02A3810463
Fingerprint (SHA256)	74ABF2AA3B2E51D43B3FA5589E4891CE10DB594BB3 AECADF476FAD2DB4DE54DC

Name of Certification Authority	Cybertrust DeviceiD Public CA G2s
Serial Number of Certification Authority Certificate	23000001
Validity Period	October 16, 2013 to November 16, 2028
Key Length	2048 bit
Signature Algorithm	SHA1withRSA
Fingerprint (SHA1)	22E8663A595B2F9A1A434AC02CBEC57AEF140DD1
Fingerprint (SHA256)	3CCE76441D13B178F22417688739CF6DA4BAAFC9AD A393EC6FE6B13A7DCD5AF8

Name of Certification Authority	Cybertrust DeviceiD Public CA G2k
Serial Number of Certification Authority Certificate	24000001
Validity Period	October 17, 2013 to November 17, 2028
Key Length	2048 bit
Signature Algorithm	SHA1withRSA
Fingerprint (SHA1)	7D88E410CCBB91D767BD9B9026083B0FAA0E6542
Fingerprint (SHA256)	D4828CD0DBB1B2781E5EFB9F4FF381C9392183806E3E1F501603807BF5E24D14

Name of Certification Authority	Cybertrust DeviceiD Public CA G2is
Serial Number of Certification Authority Certificate	25000001
Validity Period	March 20, 2014 to April 20, 2029
Key Length	2048 bit
Signature Algorithm	SHA1withRSA
Fingerprint (SHA1)	55017A8F6E3F3C80AA9F9347939E0DE04FC590A7
Fingerprint (SHA256)	F8EFFBF251CE5945134FEA5277D6BEB35FBAD6A25C537A704E947E2DCC041AE6

Name of Certification Authority	Cybertrust DeviceiD Public CA G2sp
Serial Number of Certification Authority Certificate	26000001
Validity Period	December 5, 2014 to January 5, 2030
Key Length	2048 bit
Signature Algorithm	SHA1withRSA
Fingerprint (SHA1)	E2C7DFAAA61DF61D1EB580F91602DC696FAA92DD
Fingerprint (SHA256)	C30AFB5EDF2BBE20FC636C44BBFB7AE36A34AFCC3853D1AFDFAE547F528159A3

Name of Certification Authority	Cybertrust DeviceiD Public CA G2t
Serial Number of Certification Authority Certificate	27000001
Validity Period	November 27, 2015 to December 27, 2030
Key Length	2048 bit
Signature Algorithm	SHA1withRSA
Fingerprint (SHA1)	43AD48616182223BAE04C41B8AB7A4720BD1289B
Fingerprint (SHA256)	85F4F0D092C549E0124AC28F650C02558DE6D1DA0A759C6922FC45EB2185FF2B

Name of Certification Authority	Cybertrust DeviceiD Public CA G3
Serial Number of Certification Authority Certificate	30000001
Validity Period	May 27, 2015 to June 27, 2030
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	367A42BA47DD9FA6ABF5F5470D378C39036FBB30
Fingerprint (SHA256)	6E016A5DFCB26B3D5C1CFAD61A120F5FE550542DA BEDB3710513A115CED359F2

Name of Certification Authority	Cybertrust DeviceiD Public CA G3s
Serial Number of Certification Authority Certificate	33000001
Validity Period	May 27, 2015 to June 27, 2030
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	4550E29AD57EB1529473F6B17B2D413770C67762
Fingerprint (SHA256)	B7ECDC7406978E4FA9387BE69323F71631C36DA1470 B57B4FABCE1F436A5FFD9

Name of Certification Authority	Cybertrust DeviceiD Public CA G3k
Serial Number of Certification Authority Certificate	34000001
Validity Period	April 20, 2015 to May 20, 2030
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	7E4F4D1AFAB8A0212476DF11E6362EE6D5CE1C0E
Fingerprint (SHA256)	C99EEC259E53C2167F5D68A273B7815A9FADD7D5E6 42267FAFA3221E1B17C667

Name of Certification Authority	Cybertrust DeviceiD Public CA G3is
Serial Number of Certification Authority Certificate	35000001
Validity Period	July 7, 2015 to August 7, 2030
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	813E1BDEAEDB1F48E13BEB485A7655D37BE5EEC2
Fingerprint (SHA256)	2CB6593841FFC4608362E80D55A4A706CA0A43EAC96 EC40A14713B6E5AD0DD82

Name of Certification Authority	Cybertrust DeviceiD Public CA G3sp
Serial Number of Certification Authority Certificate	36000001
Validity Period	July 7, 2015 to August 7, 2030
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	D9DAEB666F1598A379AC12DFA0205E348933DE7A
Fingerprint (SHA256)	BE6998CEE98B9525D87528757676843D52B13A73744F D00DCCF94F8183179310

Name of Certification Authority	Cybertrust DeviceiD Public CA G3t
Serial Number of Certification Authority Certificate	37000001
Validity Period	November 27, 2015 to December 27, 2030
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	C973E23FC60E7231E1774A2EC7227DC4FD2405C7
Fingerprint (SHA256)	2782776C1A6FBB06D7D711487B9C17E044B3131E1717 AC4BBFEBFEC799BADB26

Name of Certification Authority	Cybertrust DeviceiD Public CA G3h
Serial Number of Certification Authority Certificate	38000001
Validity Period	December 1, 2016 to January 1, 2032
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	AFAC2D9200AA99348FABAFDF8BDD41A95E4C3E8F
Fingerprint (SHA256)	766CA12C97E7E6C40C1E8F231D094E90E3C884257C4 5B4F19E0FCD4A3F895A77

Name of Certification Authority	Cybertrust DeviceiD Public CA G3isr
Serial Number of Certification Authority Certificate	39000001
Validity Period	February 6, 2018 to March 6, 2033
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	0E5E9F28AE713F1A1845D8B062E1522B117D9197
Fingerprint (SHA256)	AA09D0753E89F4B170021F8C85CB00DBA6ECF6406A 5121D26F84F08071CD25E2

Name of Certification Authority	Cybertrust DeviceiD Education CA G3h
Serial Number of Certification Authority Certificate	3a000001
Validity Period	July 22, 2020 to August 22, 2035
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	3C65FB8EC18AEE0DF367EAC3074EA2FD8C236360
Fingerprint (SHA256)	DA241E73AEC6B7D5047861B063B9666B2D8BAE4E2E50D46BAB809C13EA12BA61

Name of Certification Authority	Cybertrust DeviceiD Public CA G3m
Serial Number of Certification Authority Certificate	3b000001
Validity Period	December 1, 2021 to January 1, 2037
Key Length	2048 bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	E18EC029F9FFC95FD5EBA1B73B91996FE4FFBA25
Fingerprint (SHA256)	145CD9955880AF92BAA2F997EAC7EF8BEB699F679290BBDE27101175E9EF22CF

Name of Certification Authority	Cybertrust DeviceiD Private CA G4pr<xxx>(*)
Serial Number of Certification Authority Certificate	(Depends on each Certificate Authority)
Validity Period	(Depends on each Certificate Authority)
Key Length	2048bit,3072 bit or 4096bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	(Depends on each Certificate Authority)
Fingerprint (SHA256)	(Depends on each Certificate Authority)

* Certification Authority for the DeviceiD Premium option. <xxx> is an identifier.

Name of Certification Authority	Cybertrust DeviceiD Premium CA G4pr<xxx>(*)
Serial Number of Certification Authority Certificate	(Depends on each Certificate Authority)
Validity Period	(Depends on each Certificate Authority)
Key Length	2048bit,3072 bit or 4096bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	(Depends on each Certificate Authority)
Fingerprint (SHA256)	(Depends on each Certificate Authority)

* Certification Authority for the DeviceiD Premium option. <xxx> is an identifier.

Furthermore, in the occurrence of using the DeviceiD Premium 3-tier CA hierarchy option, the following Certification Authority is provided as Root Certification Authority of Issuing CA for the DeviceiD Premium option, and Cybertrust manages it. Unless otherwise prescribed herein, the term "Premium Root CA" shall include the following Certification Authority.

Name of Certification Authority	Cybertrust DeviceiD Premium Root G4rt<xxx>(*)
Serial Number of Certification Authority Certificate	(Depends on each Certificate Authority)
Validity Period	(Depends on each Certificate Authority)
Key Length	2048bit,3072 bit or 4096bit
Signature Algorithm	SHA256withRSA
Fingerprint (SHA1)	(Depends on each Certificate Authority)
Fingerprint (SHA256)	(Depends on each Certificate Authority)

* Root Certification Authority for the DeviceiD Premium 3-tier CA hierarchy option.
<xxx> is an identifier.

Unless otherwise prescribed herein, Issuing CA and Premium Root CA are collectively referred to as "Certification Authorities". Furthermore, each certificate (in addition to Device ID Certificate, Network Equipment Dedicated Server Certificate, including CA Certificate, OCSP Certificate, etc.) issued by Certification Authorities will be collectively referred to as "certificate(s)".

The operation of Certification Authorities and the issuance of certificates are conducted in accordance with the following guidelines and laws and ordinances:

(i) Cybertrust Device ID Certification Practice Statement; and

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

This "Cybertrust Device ID Certification Practice Statement" ("this CPS") prescribes the requirements for Certification Authorities to operate them and issue certificates. The requirements include obligations of Certification Authorities, obligations of subscribers, and obligations of relying parties.

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

Cybertrust will not individually prescribe a certification policy ("CP") for each certificate of a subscriber, and this CPS shall include the respective CPs.

1.2 Document Name and Identification

The official name of this CPS shall be the "Cybertrust Device ID Certification Practice Statement".

1.3 PKI Participants

The Cybertrust Japan Policy Authority ("CTJ PA") decides policies such as this CPS and appoints the Supervisor of Certification Authorities.

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

1.3.1 Certification Authorities

Issuing CA and Premium Root CA set forth in "1.1 Overview" of this CPS. The Certification Authority is composed from an Issuing Authority and a Registration Authority. Certification Authorities shall be governed by the Supervisor of Certification Authorities set forth in "5.2.1 Trusted Roles" of this CPS. Furthermore, Certification Authorities shall include the Device ID Support Desk which will handle the practical operations as Certification Authorities including the revision of this CPS, registration and deletion of the Registration Authority, registration and deletion of the Registration Authority Operator, etc. and acceptance of inquiries related to this CPS, etc.

1.3.2 Registration Authorities

The Registration Authorities consists of the following.

1.3.2.1 Device ID Certificate Registration Authority

The Device ID Certificate Registration Authority is the Registration Authority of Issuing CA involved in managing the Device ID Certificate, and is operated by the Subscriber Management Organization (defined in "1.3.4 Subscriber Management Organization" of this CPS). The Device ID Certificate Registration Authority receives a request from the Subscriber Management Organization and instructs the Issuing Authority to issue or revoke the Device ID Certificate to be distributed to a subscriber by the Subscriber Management Organization.

1.3.2.2 Network Equipment Dedicated Server Certificate Registration Authority

The Network Equipment Dedicated Server Certificate Registration Authority is the Registration Authority of Issuing CA involved in managing the Network Equipment Dedicated Server Certificate and is operated by Cybertrust. The Network Equipment Dedicated Server Certificate Registration Authority receives an application for the issuance or revocation of the Network Equipment Dedicated Server Certificate from the Subscriber Management Organization as the subscriber, and, after verifying the application information, instructs the Issuing Authority to perform the foregoing procedures. The Device ID Support Desk will serve as the support desk of the Network Equipment Dedicated Server Certificate Registration Authority with which the subscriber is to submit the application.

1.3.2.3 Registration Authority of Premium Root CA

The Registration Authority of Root Certification Authority (Premium Root CA) issues Certification Authority Certificate provided for the DeviceiD Premium option and is operated by Cybertrust. The Premium Root CA is provided to the Subscriber Management Organization who uses the DeviceiD Premium 3-tier CA hierarchy option.

1.3.3 Issuing Authority

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

1.3.4 Subscriber Management Organization

The Subscriber Management Organization is an organization that causes an individual belonging to the Subscriber Management Organization, who is appointed by the Subscriber Management Organization to be in charge of filing an application for the Service ("Responsible Service Applicant"), to submit an application form of the Service to Cybertrust, and which is accepted and registered by the Device ID Support Desk upon agreeing to this CPS and the Related Rules set forth in "2.2 Publication of Certification Information" of this CPS for managing the Device ID Certificate and will manage the Device ID Certificate Registration Authority. The Subscriber Management Organization shall request the Device ID Certificate Registration Authority operating to issue the Device ID Certificate and distribute the issued Device ID Certificate to the subscriber.

Moreover, the Subscriber Management Organization may also request the Network Equipment Dedicated Server Certificate Registration Authority to issue or revoke the Network Equipment Dedicated Server Certificate for the Network Equipment that it is using or managing.

In the course of using the Certificate, the Subscriber Management Organization shall cause the subscribers and relying parties that are being independently managed by the Subscriber Management Organization to agree to and observe this CPS and the Related Rules.

1.3.5 Subscribers

1.3.5.1 Device ID Certificate Subscriber

A subscriber of the Device ID Certificate is an individual who is under the management of the Subscriber Management Organization and who will, upon installing the Device ID Certificate distributed by the Subscriber Management Organization in the device approved by the Subscriber Management Organization, use and manage such device. If it becomes necessary to suspend the use of the Device ID Certificate, the subscriber shall follow the instructions or rules of the Subscriber Management Organization.

1.3.5.2 Network Equipment Dedicated Server Certificate Subscriber

With regard to the Network Equipment Dedicated Server Certificate, the Subscriber Management Organization will be the subscriber. The subscriber shall install the Network Equipment Dedicated Server Certificate issued by Issuing CA in the Network Equipment that it is using or managing. If it becomes necessary to suspend the use of the Network Equipment Dedicated Server Certificate, the subscriber must follow this CPS and the Related Rules, such as notifying the Network Equipment Dedicated Server Certificate Registration Authority.

1.3.6 Relying Parties

A relying party is an organization or an individual which verifies the validity of certificates of Certification Authorities and subscribers in accordance with the instructions or matters prescribed by the Subscriber Management Organization, and uses or manages the device or Network Equipment, which trust the certificates for network access authentication.

1.3.7 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Issuing CA set forth in “1.1 Overview” of this CPS will issue the following certificates to subscribers.

Certificate	Usage
Device ID Certificate	(1) Authenticating the devices in which the certificate is installed (2) Other uses approved by Issuing CA
Network Equipment Dedicated Server Certificate	(1) Authenticating the opposite Network Equipment in SSL/TLS, IPsec or IEEE 802.1x network access authentication using Device ID Certificate (2) Other uses approved by Issuing CA

1.4.2 Prohibited Certificate Uses

Issuing CA prohibits the use of the certificate for any purpose other than as set forth in “1.4.1 Appropriate Certificate Uses” of this CPS.

1.5 Policy Administration

1.5.1 Organization Administering the Documents

This CPS and related regulations will be administered by Cybertrust.

1.5.2 Contact Person

Cybertrust will accept inquiries related to the Service and this CPS at the following contact information.

Contact Information
Cybertrust Japan Co., Ltd. Device ID Support Desk Business Days: Monday to Friday (excluding National Holidays, and the designated days addressed on our website including Year-End and New Year) Business Hours: 9:00 to 18:00 (Japan Standard Time) Inquiries: did_support@cybertrust.ne.jp Address: 13F SE Sapporo Bldg., 1-2 Kita 7 Nishi 1, Kita-ku, Sapporo, 060-0807

1.5.3 Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4 CPS Approval Procedures

This CPS is approved by the CTJ PA.

1.6 Definitions and Acronyms

As prescribed in Appendix A of this CPS.

2. Publication and Repository Responsibilities

2.1 Repositories

Repositories are maintained by Cybertrust.

2.2 Publication of Certification Information

Certification Authorities will publish the following information on the repositories.

(1) Publish the following information on https://www.cybertrust.co.jp/deviceid/repository:

- this CPS;
- other end user license agreements and the like related to the Service (referring to the end user license agreements published on the repository including, but not limited to, the Cybertrust Device ID End User License Agreement; "Related Rules"); and
- Issuing CA Certificate(s) (to avoid any confusion, only the Certificate of the Cybertrust DeviceiD Public CA G2 and G3 Certification Authority shall be published on the repository, and the Certificate of other Certification Authorities shall be provided individually by the Device ID Support Desk as needed).

(2) CRL to be issued by Issuing CA will be published on each of URL indicated below.

- http://crl.deviceid.ne.jp/deviceid/g2.crl
- http://crl.deviceid.ne.jp/deviceid/g2s.crl
- http://crl.deviceid.ne.jp/deviceid/g2k.crl
- http://crl.deviceid.ne.jp/deviceid/g2is.crl
- http://crl.deviceid.ne.jp/deviceid/g2sp.crl
- http://crl.deviceid.ne.jp/deviceid/g2t.crl
- http://crl.deviceid.ne.jp/deviceid/g3.crl
- http://crl.deviceid.ne.jp/deviceid/g3s.crl
- http://crl.deviceid.ne.jp/deviceid/g3k.crl
- http://crl.deviceid.ne.jp/deviceid/g3is.crl
- http://crl.deviceid.ne.jp/deviceid/g3sp.crl
- http://crl.deviceid.ne.jp/deviceid/g3t.crl
- http://crl.deviceid.ne.jp/deviceid/g3h.crl
- http://crl.deviceid.ne.jp/deviceid/g3isr.crl
- http://crl.deviceid.ne.jp/deviceid/g3hedu.crl
- http://crl.deviceid.ne.jp/deviceid/g3m.crl
- http://crl.deviceid.ne.jp/deviceid/g4pr<xxx（*1）>.crl

  *1: <xxx> is the CA identifier specified by the DeviceiD Premium option

(3) The online revocation information (OCSP) to be provided by Issuing CA will be provided on the following URL.

- http://ocsp.deviceid.ne.jp/deviceid

However, the online revocation information (OCSP) to be provided by Issuing CA of DeviceiD Premium option will be provided on the following URL.

- http://ocsp-pr.deviceid.ne.jp/deviceid

(4) CRL to be issued by the Premium Root CA will be provided on the following URL.

- http://crl.deviceid.ne.jp/deviceid/g4rtpr<xxx（*2）>.crl

  *2: <xxx> is the CA identifier specified by the DeviceiD Premium option

(5) The online revocation information (OCSP) to be provided by the Premium Root CA may be provided on the following URL.

- http://ocsp-rtpr.deviceid.ne.jp/deviceid

2.3 Time or Frequency of Publication

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

(i) this CPS and the Related Rules shall be published each time they are amended;

(ii) CRL shall be renewed and published according to the cycle prescribed in “4.9.7 CRL Issuance Frequency” of this CPS;

(iii) OCSP response shall be renewed and provided according to the cycle prescribed in “4.9.9 On-line Revocation/Status Checking Availability” of this CPS; and

(iv) the Certification Authority Certificates shall be published in accordance with “2.2 Publication of Certification Information” of this CPS at least during the validity period.

2.4 Access Controls on Repositories

Cybertrust shall not perform any access control on the repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

3.1.2 Need for Names to be Meaningful

The name included in the DN, etc. of the Certificate shall have the meaning of the subsequent paragraph.

3.1.2.1 Device ID Certificate

DN Item	Meaning
Common Name	Device Identifying Information prescribed by the Device ID Certificate Registration Authority (including, but not limited to, terminal asset management number, etc.)
Organization	<Name of the Subscriber Management Organization followed by Corporation identifier> (Note)
Organization Unit	RA operated by <Name of the Subscriber Management Organization followed by Corporation identifier> (Note)
	Name of business division, etc. prescribed by the Device ID Certificate Registration Authority *(optional item, up to 2 terms may be used)
Country	Address of business location (country)

Item of Extended Certificate	Meaning
SubjectAltName	Alternative name of the subscriber of the certificate *(optional item)

Note: With regard to the Organization, the name that specifies the Subscriber Management Organization operating the Device ID Certificate Registration Authority is indicated as the <Name of the Subscriber Management Organization followed by Corporation identifier>.

Furthermore, similarly with regard to one Organization Unit, the same name of <Name of the Subscriber Management Organization followed by Corporation identifier> is indicated after "RA operated by".

Specifically, as the <Name of the Subscriber Management Organization followed by Corporation identifier>, used are the English name of the organization (excluding indications such as "Co., Ltd.") that was uniquely prescribed by the Device ID Support Desk and the organization identifier (4-digit hex value) uniquely prescribed by the Device ID Certificate Registration Authority at the time that the Device ID Support Desk registers the Device ID Certificate Registration Authority in Issuing CA when the Subscriber Management Organization is to start using the Service.

3.1.2.2 Network Equipment Dedicated Server Certificate

DN Item	Meaning
Common Name	FQDN or IP address of the Network Equipment being used or managed by the Subscriber Management Organization
Organization	<Name of the Subscriber Management Organization followed by Corporation identifier> (Note)
Organization Unit	Department/Division Name of the Subscriber Management Organization *(optional item, up to 2 terms may be used)
State or Province	Address (state or province) of business location of the Subscriber Management Organization *(optional item)
Locality	Address (locality) of business location of the Subscriber Management Organization *(optional item)
Country	Address (country) of business location of the Subscriber Management Organization

Item of Extended Certificate	Meaning
SubjectAltName	FQDN or IP address of the Network Equipment being used or managed by the Subscriber Management Organization *(optional item, multiple terms may be used)

Note: With regard to the Organization, the name that specifies the Subscriber Management Organization to receive the issuance of the Network Equipment Dedicated Server Certificate is indicated as the <Name of the Subscriber Management Organization followed by Corporation identifier>. Specifically, the same value as the "Note" in "3.1.2.1 Device ID Certificate" of this CPS is used.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

3.1.5.1 Device ID Certificate

Issuing CA will uniquely identify the Device ID Certificate Registration Authority based on the Organization that is indicated on the Device ID Certificate. The Device ID Certificate Registration Authority must issue and manage the Device ID Certificate in a manner such that the devices approved by the Subscriber Management Organization operating the Registration Authority can be uniquely identified based on the DN.

3.1.5.2 Network Equipment Dedicated Server Certificate

Issuing CA will uniquely identify the Network Equipment based on the DN and SubjectAltName indicated on the Network Equipment Dedicated Server Certificate.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certification Authorities do not verify 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 the registration of the Registration Authority and the issuance of the certificate.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 Device ID Certificate

Based on a request from the Subscriber Management Organization, Issuing CA will generate a private key to be distributed to a subscriber of the Device ID Certificate, and distribute the generated private key in accordance with the provisions of "6.1.2 Private Key Delivery to Subscriber" of this CPS.

When a subscriber is to generate a key pair related to the certificate, since a public key, and an electronic signature based on a private key corresponding to such public key, are included in the Certificate Signing Request ("CSR") which constitutes a part of the application information from the Subscriber Management Organization, whether the CSR has been signed with the subscriber's private key is verified by validating the electronic signature using the public key included in such CSR, and whether the subscriber owns the private key is thereby determined.

3.2.1.2 Network Equipment Dedicated Server Certificate

Issuing CA shall verify that the CSR has been signed with the subscriber's private key by validating the electronic signature using the public key included in such CSR, and thereby determine that the subscriber owns the private key.

3.2.2 Verification of Subscribers

3.2.2.1 Device ID Certificate

Issuing CA shall verify the subscribers by the Device ID Certificate Registration Authority receiving a list of subscribers managing the devices and to which the Device ID Certificate is to be distributed from the Subscriber Management Organization operating the Registration Authority, together with information related to such devices approved by the Subscriber Management Organization.

3.2.2.2 Network Equipment Dedicated Server Certificate

With regard to the Network Equipment Dedicated Server Certificate, the Subscriber Management Organization as the subscriber shall cause the Responsible Service Applicant set forth in "1.3.4 Subscriber Management Organization" of this CPS to apply for the Network Equipment Dedicated Server Certificate.

Issuing CA shall verify the subscribers on grounds that the application for the issuance of the Network Equipment Dedicated Server Certificate has been submitted by the Responsible Service Applicant of the Subscriber Management Organization and that there are no deficiencies in the application information.

3.2.3 Non-verified Subscriber Information

3.2.3.1 Device ID Certificate

Issuing CA will not request the Device ID Certificate Registration Authority to verify the truthfulness or accuracy of the values included in the Common Name (CN), alternative name (SubjectAltName), and Organization Unit Name (OU) of the subscriber of the Device ID Certificate.

3.2.3.2 Network Equipment Dedicated Server Certificate

Issuing CA shall only verify the subscriber's representation regarding the truthfulness or accuracy of the values included in the Common Name (CN), alternative name (SubjectAltName), Organization Unit Name (OU), state or province (S) and locality (L) of the subscriber of the Network Equipment Dedicated Server Certificate, and will not directly verify such values.

3.2.4 Verification of Authority

Issuing CA will verify that a subscriber is authorized to receive the issuance of the certificate based on the verification by the Registration Authority set forth in "3.2.2 Verification of Subscribers" of this CPS.

3.2.5 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

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

3.3.2 Identification and Authentication for Re-Key after Revocation

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

3.4 Idenfication and Authentication for Revocation Request

3.4.1 Idenfication and Authentication for Revocation Request

3.4.1.1 Device ID Certificate

Issuing CA will verify the authentication upon the revocation request by the Device ID Certificate Registration Authority receiving a list of Device ID Certificates to be revoked from the Subscriber Management Organization operating the Registration Authority.

3.4.1.2 Network Equipment Dedicated Server Certificate

Issuing CA will verify the authentication upon the revocation request on grounds that the revocation application of the Network Equipment Dedicated Server Certificate submitted to the Network Equipment Dedicated Server Certificate Registration Authority has been made by the Responsible Service Applicant of the Subscriber Management Organization and that there are no deficiencies in the application information.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 Device ID Certificate

The Subscriber Management Organization operating the Device ID Certificate Registration Authority.

4.1.1.2 Network Equipment Dedicated Server Certificate

The Subscriber Management Organization as the subscriber of the Network Equipment Dedicated Server Certificate.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 Device ID Certificate

As indicated in "3.2 Initial Identity Validation" of this CPS, the Subscriber Management Organization shall apply for the Device ID Certificate by submitting a list of subscribers.

4.1.2.2 Network Equipment Dedicated Server Certificate

As indicated in "3.2 Initial Identity Validation" of this CPS, the Subscriber Management Organization as the subscriber of the Network Equipment Dedicated Server Certificate shall cause the Responsible Service Applicant of the Subscriber Management Organization to submit an application to the Device ID Support Desk as the support desk of the Network Equipment Dedicated Server Certificate Registration Authority. The application shall be submitted by the Responsible Service Applicant from Cybertrust's prescribed website. When submitting the application, the subscriber must represent the truthfulness and accuracy of the application information. With regard to the CSR of the Network Equipment Dedicated Server Certificate, after the Network Equipment Dedicated Server Certificate Registration Authority receives the application, the Registration Authority Operator of the Subscriber Management Organization shall separately apply for the same from Cybertrust's prescribed website.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

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

4.2.3 Time to Process Certificate Applications

Not applicable.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

4.3.1.1 Device ID Certificate Issuance Procedures

Based on a request from the Subscriber Management Organization, the Device ID Certificate Registration Authority shall instruct the Issuing Authority to issue the Device ID Certificate. Simultaneously with issuing the Device ID Certificate, the Issuing Authority shall take measures in accordance with "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CPS for notifying the issuance of the Certificate.
Issuing CA may adopt one of the three methods described below for distributing the Device ID Certificate and the private key to a subscriber:

(i) Individual distribution of key and certificate to subscribers

A subscriber of the Device ID Certificate will directly download the Device ID Certificate and the private key via the internet in accordance with the procedures required for receiving the Device ID Certificate and the private key described in the notification of issuance.

(ii) Distribution of key and certificate to subscribers via the Subscriber Management Organization

A subscriber of the Device ID Certificate will receive the Device ID Certificate and the private key via the Subscriber Management Organization. The Subscriber Management Organization will directly receive the data from the Device ID Certificate Registration Authority in the form of a medium, etc.

(iii) Individual distribution of certificate to subscribers

When a subscriber of the Device ID Certificate generated a private key, the subscriber shall directly download only the Device ID Certificate via the internet according to the procedures required for receiving the Device ID Certificate.

4.3.1.2 Network Equipment Dedicated Server Certificate Issuance Procedures

Based on a request from a subscriber of the Network Equipment Dedicated Server Certificate, the Network Equipment Dedicated Server Certificate Registration Authority shall instruct the Issuing Authority to issue the Network Equipment Dedicated Server Certificate. Simultaneously with issuing the Network Equipment Dedicated Server Certificate, the Issuing Authority shall provide the notification set forth in "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CPS to the subscriber of the Network Equipment Dedicated Server Certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

4.3.2.1 Notification of Issuance of Device ID Certificate

Issuing CA shall notify the issuance of the Device ID Certificate as prescribed below.

(i) Individual distribution of key and certificate to subscribers

Issuing CA shall notify the issuance of the Device ID Certificate to the email address of the subscriber notified by the Device ID Certificate Registration Authority to the Issuing Authority together with information concerning the procedures required for the subscriber of the Device ID Certificate to download the Device ID Certificate and the private key.

(ii) Distribution of key and certificate to subscribers via the Subscriber Management Organization

Issuing CA shall notify the issuance of the Device ID Certificate by directly delivering the Device ID Certificate and the private key to the Subscriber Management Organization. In the foregoing case, Issuing CA shall not individually notify the issuance of the Device ID Certificate to the subscribers of the Device ID Certificate.

(iii) Individual distribution of certificate to subscribers

When a subscriber of the Device ID Certificate generated a private key, Issuing CA shall not individually notify the issuance of the Device ID Certificate to the subscribers of the Device ID Certificate.

4.3.2.2 Notification of Issuance of Network Equipment Dedicated Server Certificate

After the issuance of the Network Equipment Dedicated Server Certificate, Issuing CA shall notify the issuance of the Network Equipment Dedicated Server Certificate to the subscribers. The notification shall be sent to the email address designated when the Registration Authority Operator of the Subscriber Management Organization applied for the CSR of the Network Equipment Dedicated Server Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 Device ID Certificate

Issuing CA shall take the Device ID Certificate acceptance verification procedures as prescribed below depending on the distribution method of the Certificate, etc.

(i) Individual distribution of key and certificate to subscribers

A subscriber of the Device ID Certificate shall download the Device ID Certificate and the private key related to the Device ID Certificate, upon self-certification, in accordance with the instructions in the email sent from Issuing CA based on the provisions of "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CPS. Issuing CA will deem that the subscriber of the Device ID Certificate has received the Device ID Certificate as a result of the subscriber downloading the Device ID Certificate and the private key from Cybertrust's prescribed website.

(ii) Distribution of key and certificate to subscribers via the Subscriber Management Organization

Issuing CA shall verify the acceptance of the Device ID Certificate as a result of directly delivering the Device ID Certificate and the private key to the Subscriber Management Organization. The Subscriber Management Organization must properly distribute to the Device ID Certificate and the private key to the subscriber.

(iii) Individual distribution of certificate to subscribers

When a subscriber of the Device ID Certificate generated a private key, the subscriber shall directly download only the Device ID Certificate via the internet according to the procedures required for receiving the Device ID Certificate. Issuing CA will deem that the subscriber of the Device ID Certificate has received the Device ID Certificate as a result of the subscriber downloading the Device ID Certificate from Cybertrust's prescribed website.

4.4.1.2 Network Equipment Dedicated Server Certificate

A subscriber of the Network Equipment Dedicated Server Certificate shall download the Network Equipment Dedicated Server Certificate in accordance with the contents of the notification recorded in the email sent from Issuing CA based on the provisions of "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CPS. Issuing CA will deem that the subscriber of the Network Equipment Dedicated Server Certificate has received the Network Equipment Dedicated Server Certificate as a result of the subscriber downloading the Network Equipment Dedicated Server Certificate from Cybertrust's prescribed website.

4.4.2 Publication of the Certificate by the CA

Issuing CA shall not publish a subscriber's certificate.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Issuing CA shall not notify the issuance of certificates other than those based on the provisions of "4.3.2 Notification to Subscriber by the CA of Issuance of Certificate" of this CPS.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

4.5.1.1 Device ID Certificate

A subscriber of the Device ID Certificate shall install the private key and the Device ID Certificate in the device approved by the Subscriber Management Organization so that the private key and the Device ID Certificate will be used only for the usage set forth in "1.4.1 Appropriate Certificate Uses" of this CPS. Furthermore, the private key and the Device ID Certificate may be used only in the device for which installation was approved and must not be used in other devices. Other obligations of the subscriber regarding the use of the private key and the Device ID Certificate are set forth in "9.6.3 Representations and Warranties of Subscribers" of this CPS, and the subscriber of the Device ID Certificate must observe such obligations pursuant to the instructions or rules of the Subscriber Management Organization.

4.5.1.2 Network Equipment Dedicated Server Certificate

A subscriber of the Network Equipment Dedicated Server Certificate shall install the Network Equipment Dedicated Server Certificate in the Network Equipment to which the Common Name (CN) or alternative name (SubjectAltName) corresponds so that the Network Equipment Dedicated Server Certificate will be used only for the usage set forth in "1.4.1 Appropriate Certificate Uses" of this CPS. The Network Equipment Dedicated Server Certificate may be used only in the corresponding Network Equipment, and the subscriber must not use the Network Equipment Dedicated Server Certificate in other Network Equipment. Other obligations of the subscriber regarding the use of the Network Equipment Dedicated Server Certificate are set forth in "9.6.3 Representations and Warranties of Subscribers" of this CPS, and the subscriber of the Network Equipment Dedicated Server Certificate must observe such obligations.

4.5.2 Relying Party Public Key and Certificate Usage

A relying party shall verify the validity of the certificates of Certification Authorities and the subscriber in accordance with the instructions or rules of the Subscriber Management Organization, and shall configure and manage the devices or Network Equipment so that the foregoing certificates are relied upon.

Other obligations of a relying party regarding the use of the public key and certificates are set forth in "9.6.5 Relying Partiy Representations and Warranties" of this CPS, and the relying party must observe such obligations pursuant to the instructions or rules of the Subscriber Management Organization.

4.6 Certificate Renewal

Issuing CA shall not allow the renewal of a certificate that does not involve the renewal of a key pair.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

4.7.1.1 Device ID Certificate

The Device ID Certificate Registration Authority shall renew and issue the Device ID Certificate of a subscriber whose renewal of the Device ID Certificate was approved by the Subscriber Management Organization operating the Registration Authority; provided, however, that Issuing CA shall generate a new key pair upon renewing the Device ID Certificate. In cases where the subscriber has generated a key pair and Issuing CA has delivered only the certificate, the subscriber must generate a new key pair.

4.7.1.2 Network Equipment Dedicated Server Certificate

When renewing the Network Equipment Dedicated Server Certificate, a subscriber of the Network Equipment Dedicated Server Certificate must generate a new key pair.

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The provisions of “4.4.1 Conduct Constituting Certificate Acceptance” of this CPS shall apply correspondingly.

4.7.6 Publication of the Re-keyed Certificate by the CA

The provisions of “4.4.2 Publication of the Certificate by CA” of this CPS 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 CPS shall apply correspondingly.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

4.8.1.1 Device ID Certificate

The Device ID Certificate Registration Authority shall not accept a request for modifying a previously issued Device ID Certificate. If it is necessary to modify the information of the Device ID Certificate, a subscriber of the Device ID Certificate shall follow the instructions or rules of the Subscriber Management Organization, such as by contacting the organization that authorized the use or management of the Device ID Certificate.

4.8.1.2 Network Equipment Dedicated Server Certificate

The Network Equipment Dedicated Server Certificate Registration Authority shall not accept a request for modifying a previously issued Network Equipment Dedicated Server Modification of Certificate. If it is necessary to modify the information of the Network Equipment Dedicated Server Certificate, a subscriber of the Network Equipment Dedicated Server Certificate shall individually submit a revocation application and a new application of the Network Equipment Dedicated Server Certificate.

4.8.2 Who may Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reason of Revocation by Registration Authority

In the occurrence of any one of the following events, the Registration Authority shall revoke the certificate for which it requested the Issuing Authority to issue at the time that such event is discovered:

(i) the Subscriber Management Organization terminats the use of options related to certificate issuance; thus the certificate needs to be revoked;

(ii) the Registration Authority learns, based on reasonable evidence, that a subscriber's private key has been compromised or there is a possibility thereof;

(iii) the Registration Authority learns, based on reasonable evidence, that the contents of the certificate are contrary to facts;

(iv) the Registration Authority learns, based on reasonable evidence, that the certificate is being used without authorization;

(v) the Registration Authority learns, based on reasonable evidence, that the certificate is being issued to a person other than a subscriber without authorization; or

(vi) the Registration Authority learns, based on reasonable evidence, that the certificate is being issued in breach of this CPS or the Related Rules.

4.9.1.2 Reason of Revocation by Device ID Support Desk

In the occurrence of any one of the following events, the Device ID Support Desk may instruct the Issuing Authority to revoke the corresponding certificate at the time that such event is discovered; provided, however, that, with regard to (vi) below, the Device ID Support Desk may instruct the revocation on the day that Issuing CA separately provides a prior notice before termination of operations:

(i) the use of the Service or the use of options related to the certificate by the Subscriber Management Organization is terminated;

(ii) the Registration Authority or the Subscriber Management Organization operating the Registration Authority breaches this CPS or the Related Rules and, even after the Device ID Support Desk sends a notice demanding the correction of said breach, the breach is not corrected even after the lapse of seven (7) days from the dispatch of the foregoing notice;

(iii) the Device ID Support Desk learns, based on reasonable evidence, that the certificate is being issued in a manner that is not based on the instructions of the Registration Authority, or in a manner that differs from the instructions of the Registration Authority;

(iv) the Device ID Support Desk learns that Certification Authority's private key has been compromised or there is a possibility thereof;

(v) Certification Authorities issues the certificate without conforming to this CPS; or

(vi) Certification Authorities terminates its certification operations.

4.9.1.3 Reason of Revocation by Subscriber Management Organization

If the Subscriber Management Organization acknowledges that it is necessary to revoke the Device ID Certificate that was distributed to a subscriber being managed by the Subscriber Management Organization and the Network Equipment Dedicated Server Certificate that the Subscriber Management Organization uses (including, but not limited to, any one of the following events), the Subscriber Management Organization shall immediately request the corresponding Registration Authority to revoke the corresponding certificate:

(i) the Subscriber Management Organization will discontinue the use of the device or the Network Equipment in which the certificate has been installed;

(ii) the Subscriber Management Organization will discontinue the use of the certificate in the device or the Network Equipment;

(iii) the Subscriber Management Organization learns, based on reasonable evidence, that a private key of the device or the Network Equipment has been compromised or there is a possibility thereof;

(iv) the Subscriber Management Organization learns, based on reasonable evidence, that the contents of the certificate are contrary to facts;

(v) the Subscriber Management Organization learns, based on reasonable evidence, that the certificate is being used without authorization;

(vi) the Subscriber Management Organization learns, based on reasonable evidence, that the certificate is being issued to a person other than a subscriber without authorization; or

(vii) the Subscriber Management Organization learns, based on reasonable evidence, that the certificate is being issued or used in breach of this CPS or the Related Rules.

4.9.1.4 Reason of Revocation by Subscriber

(i) Device ID Certificate

If a subscriber of the Device ID Certificate acknowledges that it is necessary to revoke the Device ID Certificate (including, but not limited to, any one of the following events), the subscriber shall follow the instructions or rules of the Subscriber Management Organization, such as by contacting the organization that authorized the use or management of the Device ID Certificate.

a a subscriber will discontinue the use of the device in which the Device ID Certificate was installed;

b a subscriber will discontinue the use of the Device ID Certificate in the device;

c a subscriber learns, based on reasonable evidence, that a private key installed in the device has been compromised or there is a possibility thereof;

d a subscriber learns, based on reasonable evidence, that the contents of the Device ID Certificate are contrary to facts;

e a subscriber learns, based on reasonable evidence, that the Device ID Certificate is being used without authorization; or

f a subscriber learns, based on reasonable evidence, that the Device ID Certificate is being used in breach of this CPS or the Related Rules.

(ii) Network Equipment Dedicated Server Certificate

The provisions of "4.9.1.3 Reason of Revocation by Subscriber Management Organization" of this CPS shall apply to the reason of revocation by a subscriber of the Network Equipment Dedicated Server Certificate.

4.9.2 Who Can Request Revocation

Persons who may request revocation of a certificate shall be as follows.

As indicated in "4.9.1.2 Reason of Revocation by Device ID Support Desk" of this CPS, if the Device ID Support Desk deems necessary, the Device ID Support Desk may instruct the Issuing Authority to revoke a certificate.

4.9.2.1 Device ID Certificate

Subscriber Management Organization

4.9.2.2 Network Equipment Dedicated Server Certificate

Subscriber Management Organization

4.9.3 Procedure for Revocation Request

The Registration Authority shall revoke a certificate based on a revocation request from the requester approved for each certificate.

Furthermore, as indicated in "4.9.1.2 Reason of Revocation by Device ID Support Desk" of this CPS, if the Device ID Support Desk deems necessary, the Device ID Support Desk may instruct the Issuing Authority to revoke a certificate.

4.9.4 Revocation Request Grace Period

When a party requesting revocation acknowledges that revocation is required, such party shall promptly submit a revocation request.

4.9.5 Time within Which CA Must Process the Revocation Request

The Issuing Authority shall promptly revoke the certificate after receiving the revocation requests.

4.9.6 Revocation Checking Requirement for Relying Parties

The relying parties shall confirm the certificate revocation with CRL or OCSP created by Certification Authorities.

4.9.7 CRL Issuance Frequency

Issuing CA issues CRL in a cycle of no grater than 1hours.
Premium Root CA issues CRL in a cycle of no grater than 13 months.

4.9.8 Maximum Latency for CRLs

The validity period of Issuing CA's CRL is 168 hours. Issuing CA shall publish the latest CRL in the repository no later than one (1) hour after the revocation of the certificate; provided, however, that, based on the determination of Issuing CA, CRL may be issued or published beyond the foregoing validity period or delay time.

The validity period of Premium Root CA's CRL is up to 13 months. Premium Root CA shall publish the latest CRL in the repository no later than one (1) business day after the revocation of the certificate that is issued by itself; provided, however, that, based on the determination of the Premium Root CA, CRL may be issued or published beyond the foregoing validity period or delay time.

4.9.9 On-line Revocation/Status Checking Availability

Issuing CA shall provide revocation information based on OCSP, in addition to CRL. However, if the signature algorithm is SHA1withRSA or the subscriber management organization has agreed to use the Premium Option with Device ID, the certification authority in question will not provide revocation information via OCSP. Issuing CA's validity period of OCSP response is 168 hours. Issuing CA shall renew OCSP response based on the latest CRL published on the repository; provided, however, that, based on the determination of Issuing CA, the validity period of OCSP response may exceed the foregoing validity period or cycle.

Premium Root CA shall provide revocation information based on OCSP, in addition to CRL. However, if the subscriber management organization has agreed to use the Premium Option with Device ID, the certification authority in question will not provide revocation information via OCSP. Premium Root CA's validity period of OCSP response is no grater than 13 months. Premium Root CA shall renew OCSP response based on the latest CRL published on the repository; provided, however, that, based on the determination of Premium Root CA, the validity period of OCSP response may exceed the foregoing validity period or cycle.

4.9.10 On-line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

Not applicable.

4.9.13 Circumstances for Suspension

Issuing CA will permit the suspension of certificates.

The Issuing Authority of Issuing CA shall receive instructions for suspending the Certificate from the Registration Authority of Issuing CA, register the information of the Certificate to be suspended in CRL, as well as receiving instructions for terminating the suspension of the Certificate, and delete the information of the Certificate, which was registered in CRL, from CRL.

Premium Root CA shall not permit the suspension of certificates.

4.9.14 Who Can Request Suspension

The provisions of "4.9.2 Who Can Request Revocation" of this CPS shall apply correspondingly.

4.9.15 Procedure for Suspension Request

The provisions of "4.9.3 Procedure for Revocation Request" of this CPS shall apply correspondingly.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

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

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

When the certificate that was issued to subscriber who underwent the verification described in “3.2.2 Verification of Subscribers” of this CPS expires, the subsription will end. Or, the subsription will end when the revocation of the certificate occurs based on “4.9.1 Circumstances for Revocation” of this CPS.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The system that constitutes Certification Authorities (referring to the system for providing the Service managed by Cybertrust, but not including the terminals and the like used by the Registration Authority for performing the certification operations; "Certification Authority Systems") shall be installed in a facility that is not easily affected by earthquakes, fires, floods and other disasters ("Facility"; unless otherwise prescribed herein, the term "Facility" shall include the main site and the backup site set out in "5.1.9 Off-site Backup" of this CPS). The Facility shall undergo architectural measures for preventing earthquakes, fires, floods and other disasters as well as preventing trespassing. Information regarding the location of Certification Authorities shall not be indicated outside or inside the building where the Facility is located.

5.1.2 Physical Access

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

The Facility shall be monitored with a monitoring system 24/7.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

A water leakage detector shall be installed in the particularly important rooms in the Facility, and waterproofing measures shall be taken for the ceiling and floor.

5.1.5 Fire Prevention and Protection

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

5.1.6 Anti-earthquake Measures

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

5.1.7 Media Storage

In the Facility, mediums containing the backup data of the Certification Authority Systems and related documents shall be archived in a room in which only authorized personnel permitted to use such mediums and documents can enter.

5.1.8 Waste Disposal

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

5.1.9 Off-site Backup

Originals and copies of important assets required for the restoration of the private key and system of Certification Authorities shall be stored in the main site, and shall not be stored in the backup site.

However, originals and copies of important assets required for the restoration of the OCSP server shall be stored in the main site and also in a remote backup site. The safe of the backup site shall be managed by being locked by multiple persons, and the opening of the safe shall be recorded.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

5.2.1.1 Certification Authority Supervisor

The Supervisor of Certification Authorities shall be appointed by Cybertrust and governs Certification Authorities.

5.2.1.2 Issuing Authority Supervisor

The Issuing Authority Supervisor shall be appointed by Cybertrust and controls the operations of Issuing Authorities of Certification Authorities.

5.2.1.3 Issuing Authority System Administrator

The Issuing Authority System Administrator shall maintain and control the Certification Authority Systems under the control of the Issuing Authority Supervisor.

5.2.1.4 Issuing Authority Operator

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

5.2.1.5 Registration Authority Operator Supervisor (RA Operator Supervisor)

(i) Device ID Certificate

The Registration Authority Operator Supervisor (RA Operator Supervisor) of the Device ID Certificate shall be a person appointed by the Subscriber Management Organization among the employees or officers of the Subscriber Management Organization and registered and accepted by the Device ID Support Desk, and shall manage the registration operations of the Device ID Certificate of Issuing CA.

(ii) Network Equipment Dedicated Server Certificate

The Registration Authority Operator Supervisor (RA Operator Supervisor) of the Network Equipment Dedicated Server Certificate shall be a person appointed by Cybertrust and shall manage the registration operations of the Network Equipment Dedicated Server Certificate of Issuing CA.

5.2.1.6 Registration Authority Operator (RA Operator)

(i) Device ID Certificate

The Registration Authority Operator (RA Operator) of the Device ID Certificate shall be a person appointed by the Subscriber Management Organization and registered and accepted by the Device ID Support Desk, and shall give instructions to the Issuing Authority for issuing or revoking the Device ID Certificate of a subscriber acknowledged by the Subscriber Management Organization under the management of the Registration Authority Operator Supervisor of the Device ID Certificate.

(ii) Network Equipment Dedicated Server Certificate

The Registration Authority Operator (RA Operator) of the Network Equipment Dedicated Server Certificate shall be a person appointed by Cybertrust, and shall give instructions to the Issuing Authority for issuing or revoking the Network Equipment Dedicated Server Certificate under the management of the Registration Authority Operator Supervisor of the Network Equipment Dedicated Server Certificate.

5.2.2 Number of Persons Required Per Task

Certification Authorities shall appoint two or more Issuing Authority System Administrators.

5.2.3 Identification and Authentication for Each Role

Certification Authorities shall establish the entrance authority of the respective rooms in the Facility and the access authority to the Certification Authority Systems in accordance with the respective roles. For entry into the respective rooms and access to the system, measures such as an entrance/exit card, biometric identification, certificate, ID and password are taken independently or in combination for verifying and authenticating the identification and authority.

5.2.4 Roles Requiring Separation of Duties

Issuing CA will not allow the concurrent serving of the Device ID Certificate Registration Authority and the Issuing Authority, and Certification Authorities will not allow the Supervisor of Certification Authorities to concurrently serve another role.

The Registration Authority shall not approve the concurrent serving of the Registration Authority Operator Supervisor and the Registration Authority Operator.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The Certification Authority Staff (excluding the Registration Authority Operator Supervisor and the Registration Authority Operator of the Device ID Certificate; hereinafter the same) shall be hired, appointed and assigned based on the recruitment standards to be separately set forth by Cybertrust.

The appointment and assignment of the Registration Authority Operator Supervisor and the Registration Authority Operator of the Device ID Certificate shall be pursuant to the standards and rules of the Subscriber Management Organization that has appointed such Registration Authority Operator Supervisor and Registration Authority Operator.

5.3.2 Background Checks Procedures

Not applicable.

5.3.3 Training Requirements

Certification Authorities shall implement necessary training requirements and procedures to all employees of Cybertrust who will be assigned as the Certification Authority Staff.

With regard to the implementation of training requirements and procedures to the Registration Authority Operator Supervisor and the Registration Authority Operator of the Device ID Certificate, when the Subscriber Management Organization that appointed such Registration Authority Operator Supervisor and Registration Authority Operator of the Device ID Certificate deems necessary, the Subscriber Management Organization may reach a separate agreement with Cybertrust, and Cybertrust may implement such training requirements and procedures.

5.3.4 Retraining Frequency and Requirements

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

(i) when this CPS and the Related Rules are amended, and the CTJ PA, Certification Authority Supervisor, Issuing Authority Supervisor, or Registration Authority Supervisor of the Network Equipment Dedicated Server Certificate deems necessary;

(ii) when the Certification Authority Systems is changed, and the CTJ PA, Certification Authority Supervisor, Issuing Authority Supervisor, or Registration Authority Supervisor of the Network Equipment Dedicated Server Certificate deems necessary;

(iii) when the CTJ PA, Certification Authority Supervisor, Issuing Authority Supervisor, or Registration Authority Supervisor of the Network Equipment Dedicated Server Certificate deems necessary.

With regard to the retraining of the Registration Authority Operator Supervisor and the Registration Authority Operator of the Device ID Certificate, when the Subscriber Management Organization deems necessary such as when the appointee is changed, the Subscriber Management Organization may reach a separate agreement with Cybertrust, and Cybertrust may implement such retraining.

5.3.5 Job Rotation Frequency and Sequence

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

Not applicable to the Registration Authority Operator Supervisor and the Registration Authority Operator of the Device ID Certificate.

5.3.6 Sanction for Unauthorized Actions

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

When the Device ID Support Desk learns that the Registration Authority Operator Supervisor or the Registration Authority Operator of the Device ID Certificate conducted an act that is in breach of this CPS and the Related Rules, the Device ID Support Desk shall send a notice to the corresponding Registration Authority requesting the correction of such breach. If the breach is not corrected even after the lapse of 7 days after the dispatch of the foregoing notice, the Support Desk shall take necessary measures such as terminating the registration as the Device ID Certificate Registration Authority.

5.3.7 Independent Contractor Requirements

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

When the Subscriber Management Organization is to assign a Contract Employee, for which the Subscriber Management Organization is responsible for managing, as the Registration Authority Operator of the Device ID Certificate, the Subscriber Management Organization shall execute an agreement with such Contract Employee which prescribes the description of job duties, confidentiality obligations and penalties, demand that Contract Employee to observe this CPS and the Related Rules, and obtain the consent of that Contract Employee to the effect of observing this CPS and the Related Rules.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

(i) records in the Certification Authority Systems (including records of issue/revocation requests by the Registration Authority);

(ii) records regarding network security of the Certification Authority Systems;

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

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

5.4.2 Frequency of Processing Log

Certification Authorities shall verify the monitoring logs prescribed in "5.4.1 Types of Events to be Recorded" of this CPS on a monthly basis or as needed.

5.4.3 Retention Period for Audit Log

With regard to "5.4.1 Types of Events to be Recorded" (i), records shall be archived for at least 1 year after the expiration of the validity period of the issued certificate.

Other records shall be archived at least 3 years.

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (internal vs. external)

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

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

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

5.5 Records Archival

5.5.1 Types of Records Archived

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

(i) Self-signed Certificate, Certification Authority Certificate;

(ii) subscriber's certificate;

(iii) CRL;

(iv) internal audit report;

(v) Service request forms and other documents received from the Subscriber Management Organization; and

(vi) this CPS and the Related Rules.

5.5.2 Retention Period for Archive

Certification Authorities shall archive the records prescribed in "5.5.1 Types of Records Archived" of this CPS for at least 1 year beyond the validity period of the relevant certificate.

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-stamping of Records

In relation to "5.5.1 Types of Records Archived" of this CPS, Certification Authorities shall record the drafting date or processing date on forms and the like. If the date alone will lack authenticity as a record, the time should also be recorded. The issued date and time for certificates of Certification Authorities and the subscribers shall also be recorded. The Certification Authority Systems shall undergo necessary measures for recording the accurate date and time of the issued certificates and monitoring logs.

5.5.6 Archive Collection System (internal or external)

In relation to "5.5.1 Types of Records Archived" of this CPS, the certificates shall automatically be collected based on the function of the Certification Authority Systems. Other paper mediums shall be collected by the Certification Authority Staff.

5.5.7 Procedures to Obtain and Verify Archive Information

In relation to "5.5.1 Types of Records Archived" of this CPS, Certification Authorities shall limit persons authorized to acquire and peruse records to the Certification Authority Staff, the auditor and persons authorized by the CTJ PA. Validation regarding the legibility of records shall be implemented as needed.

5.6 Key Changeover

Certification Authorities will renew the key pair of Certification Authorities at least every 10 years.

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Excluding cases that are attributable to the Issuing Authority, Cybertrust shall treat the suspension of the Service caused by the compromise of the Certification Authority's private key as a force majeure event and will not guarantee the time required for resuming the Service.

If the Certification Authority's private key is compromised, the Device ID Support Desk shall notify the relevant Subscriber Management Organization of such fact and additionally publish such fact on the repository of Certification Authorities. Immediately after receiving the foregoing notice from the Device ID Support Desk, the Subscriber Management Organization shall notify such fact to the subscribers and relying parties being managed by the Subscriber Management Organization.

Certification Authorities shall implement the measures listed above, and endeavour to resume the Service by executing the following:

(i) discontinuation of certification operations using the compromised private key;

(ii) revocation of all certificates;

(iii) investigation of the cause of compromise;

(iv) formulation of proposed remedial measures and evaluation/approval thereof by the CTJ PA;

(v) execution of remedial measures;

(vi) assessment on appropriateness of resuming business operations;

(vii) generation of new key pairs and issuance of certificates;

(viii) resumption of certification operations (including notification to subscribers and relying parties); and

(ix) reissuance of certificates.

When Certification Authorities suffers from a disaster, Certification Authorities shall exert efforts to resume the Service based on the provisions of "5.7.4 Business Continuity Capabilities after a Disaster" of this CPS.

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

When hardware, software or data is destroyed, Certification Authorities shall perform recovery operations and continue performing the certification operations by using the backup hardware, software or data.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 Device ID Certificate

In the event the private key is compromised, or suspected of being compromised, a subscriber of the Device ID Certificate shall follow the instructions or rules of the Subscriber Management Organization, such as contacting the Subscriber Management Organization of the occurrence of such event, as described in "4.9.1 Circumstances for Revocation" of this CPS.

5.7.3.2 Network Equipment Dedicated Server Certificate

In the event the private key used in the Network Equipment is compromised, or suspected of being compromised, a subscriber of the Network Equipment Dedicated Server Certificate shall suspend the use of the certificate corresponding to the Network Equipment, and must apply for the revocation of the certificate with the Network Equipment Dedicated Server Certificate Registration Authority as indicated in "4.9.1 Circumstances for Revocation" of this CPS.

5.7.4 Business Continuity Capabilities after a Disaster

Cybertrust shall treat the suspension of the Service caused by disasters as a force majeure event, and will not guarantee the time required for resuming the Service.

If the Service is suspended due to disasters, the Device ID Support Desk shall notify the Subscriber Management Organization of such fact and additionally publish such fact on Cybertrust's website. Immediately after receiving the foregoing notice from the Device ID Support Desk, the Subscriber Management Organization shall notify such fact to the relevant subscribers and relying parties.

Cybertrust managing the Certification Authority shall implement the measures listed above, and additionally investigate the disaster situation and formulate a recovery policy based on the investigation results, and the Issuing Authority, the Registration Authority, and the Device ID Support Desk shall implement the recovery work in accordance with the formulated recovery policy.

5.8 CA or RA Termination

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

Information concerning the issue/revocation requests of the Certificate held by the Certification Authority shall be abolished, and this shall be announced on Cybertrust's website after the termination of operations.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pair used in Certification Authorities and OCSP server will be generated based on instructions of the Supervisor of Certification Authorities by multiple Issuing Authority System Administrators under the control of the Issuing Authority Supervisor. Upon generating the key pair of Certification Authorities, a private key cryptographic module ("HSM") that satisfies the FIPS 140 Level 4 standard shall be used. Upon generating the key pair used in an OCSP server, the software that satisfies the FIPS 140 Level 1 standard shall be used.

6.1.2 Private Key Delivery to Subscriber

6.1.2.1 Device ID Certificate

With regard to the Device ID Certificate, Issuing CA shall generate a private key of the Device ID Certificate based on the request of the Subscriber Management Organization, and distribute the private key to a subscriber upon taking measures for ensuring the confidentiality and safety of the private key. When a subscriber is to generate a key pair related to the certificate, the subscriber shall generate the key pair and manage and preserve the private key under its own responsibility, and Issuing CA shall not distribute the key.

6.1.2.2 Network Equipment Dedicated Server Certificate

With regard to the Network Equipment Dedicated Server Certificate, Issuing CA shall not distribute the private key thereof. The private key shall be independently generated by the subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 Device ID Certificate

Issuing CA will not accept the delivery of a public key of the Device ID Certificate from a subscriber.

6.1.3.2 Network Equipment Dedicated Server Certificate

The public key of the Network Equipment Dedicated Server Certificate shall be included in the CSR which is a part of the application information from the subscriber.

6.1.4 CA Public Key Delivery to Relying Parties

Certification Authorities will not deliver the public key of Certification Authorities to relying parties. The Self-signed Certification Authority Certificate which includes the public key of Issuing CA will be published on the repository in accordance with "2.2 Publication of Certification Information" of this CPS.

6.1.5 Key Sizes

The signature algorithm and key length of the certificates issued by Issuing CA shall be pursuant to the following table.

Certificate	Signature Algorithm	Key Length
Self-signed Certificate	SHA1 with RSA or SHA256 with RSA	2048 bits or greater
Device ID Certificate	SHA1 with RSA or SHA256 with RSA	2048 bits or greater (Note)
Network Equipment Dedicated Server Certificate	SHA1 with RSA or SHA256 with RSA	2048 bits or greater(Note)
OCSP Server Certificate	SHA1 with RSA or SHA256 with RSA	2048 bits

Note: 1024 bits will be allowed only when the device is not compatible with the 2048-bit key length.

The signature algorithm and key length of the certificates issued by Premium Root CA shall be pursuant to the following table.

Certificate	Signature Algorithm	Key Length
Self-signed Certificate	SHA256 with RSA	2048 bits or greater
Certification Authority Certificate	SHA1 with RSA or SHA256 with RSA	2048 bits or greater
OCSP Server Certificate	SHA1 with RSA or SHA256 with RSA	2048 bits

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

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

The key usage of the Certificate issued by Issuing CA shall be pursuant to the following table.

Certificate	Key Usage
Self-signed Certificate	Certificate Signing, CRL Signing
Device ID Certificate	Digital Signature, Key Encipherment
Network Equipment Dedicated Server Certificate	Digital Signature, Key Encipherment
OCSP Server Certificate	Digital Signature

The key usage of the Certificate issued by Premium Root CA shall be pursuant to the following table.

Certificate	Key Usage
Self-signed Certificate	Certificate Signing, CRL Signing
Certification Authority Certificate	Certificate Signing, CRL Signing
OCSP Server Certificate	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 Certification Authorities shall be the HSM that satisfies the FIPS 140 Level 4 standard. The HSM will be controlled by the Issuing Authority.

The key pair used in an OCSP server will be controlled based on the HSM that satisfies the FIPS 140 Level 1 standard. The OCSP server will be controlled by the Issuing Authority.

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

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

6.2.3 Private Key Escrow

Certification Authorities will not deposit the private key used by Certification Authorities and the OCSP server or deposit the private key of subscribers.

6.2.4 Private Key Backup

The Issuing Authority System Administrator shall back up the private key of Certification Authorities. The private key backed up from the HSM shall be encrypted and then divided into multiple pieces, and safely archived in a lockable safe. When the private key needs to be restored due to a malfunction of the HSM or other reasons, the Issuing Authority System Administrator shall restore the private key by using the backup.

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

6.2.5 Private Key Archive

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

Certification Authorities shall not transfer a copy of the private key to be used by Certification Authorities and the OCSP server outside the Facility.

When the private key of the OCSP server needs to be restored, the Issuing Authority System Administrator shall do so using the system backup stored in the main site or the backup site; provided, however, that, based on the approval of the Supervisor of Certification Authorities, there may be cases where the corresponding certificate is revoked and a new private key is generated.

6.2.7 Private Key Storage on Cryptographic Module

The private key of Certification Authorities shall be generated, encrypted and maintained in the HSM.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the certificates issued by Issuing CA shall be pursuant to the following table.

Certificate	Validity Period
Self-signed Certificate	No greater than 182 months
Device ID Certificate	No greater than 62 months
Network Equipment Dedicated Server Certificate	No greater than 62 months (Note)
OCSP Server Certificate	No greater than 25 months

Note: The validity period of certificates issued by Issuing CA in which the signature algorithm method is compliant with SHA256withRSA or higher on September 12, 2019 onward shall be No greater than 26 months.

The validity period of the certificates issued by Premium Root CA shall be pursuant to the following table.

Certificate	Validity Period
Self-signed Certificate	No greater than 182 months
Certification Autnority Certificate	No greater than 182 months
OCSP Server Certificate	No greater than 25 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

(i) authentication of authority of the operator;

(ii) identification and authentication of the operator;

(iii) acquisition of operation logs for important system operations;

(iv) setup of appropriate passwords and periodical modification thereof; and

(v) backup and recovery.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

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

6.8 Time-stamping

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Matters regarding the Self-signed Certificate, Device ID Certificate, Network Equipment Dedicated Server Certificate and OCSP Server Certificate are set forth in Appendix B.

7.1.2 Certificate Extensions

Matters regarding the Self-signed Certificate, Device ID Certificate, Network Equipment Dedicated Server Certificate and OCSP Server Certificate are set forth in Appendix B.

7.1.3 Algorithm Object Identifiers

Matters regarding the Self-signed Certificate, Device ID Certificate, Network Equipment Dedicated Server Certificate and OCSP Server Certificate are set forth in Appendix B.

7.1.4 Name Forms

Matters regarding the Self-signed Certificate, Device ID Certificate, Network Equipment Dedicated Server Certificate and OCSP Server Certificate are set forth in Appendix B.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

The certificate policy object identifier of the Certificate issued by Issuing CA shall be pursuant to the following table.

Certificate	Certificate Policy Object Identifier
Device ID Certificate	1.2.392.00200081.1.11.1
Network Equipment Dedicated Server Certificate	1.2.392.00200081.1.11.2

7.1.7 Use of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Matters regarding the Self-signed Certificate, Certification Authority Certificate, Device ID Certificate and Network Equipment Dedicated Server Certificate are set forth in Appendix B.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

7.2.1 Version Number(s)

Matters regarding the CRL issued by Certification Authorities are set forth in Appendix B.

7.2.2 CRL and CRL Entry Extensions

Matters regarding the CRL issued by Certification Authorities are set forth in Appendix B.

7.3 OCSP Profile

7.3.1 Version Number(s)

Matters regarding the OCSP Server Certificate are set forth in Appendix B.

7.3.2 OCSP Extensions

Matters regarding the OCSP Server Certificate are set forth in Appendix B.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

If doubts arise in the certification operations, Certification Authorities may cause the auditor set forth in “8.2 Identity/Qualifications of Assessor” of this CPS to audit all or a part of the Issuing Authority and the Registration Authority.

The Registration Authority must cooperate with the audit to be carried out by Cybertrust.

8.2 Identity/Qualifications of Assessor

The audit of Certification Authorities shall be carried out by a party possessing necessary knowledge and experience authorized by the CTJ PA.

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The scope of audit shall be the scope of the certification operations of Certification Authorities that are being implemented in accordance with this CPS.

8.5 Actions Taken as a Result of Deficiency

Identified matters that are discovered in the audit will be reported to the CTJ PA and the Supervisor of Certification Authorities.

When it is determined that corrective action against the Issuing Authority or the Network Equipment Dedicated Server Certificate Registration Authority is required, such corrective action shall be taken under the control of the Issuing Authority Supervisor.

When it is determined that corrective action against the Device ID Certificate Registration Authority, the Device ID Support Desk shall send a notice to the Registration Authority requesting the implementation of such corrective action, and the Registration Authority must comply with such request.

8.6 Communication of Results

The results of audit are disclosed only to any third parties authorized by the CTJ PA (including those who are entitled to disclosure requests by law, regulation, or agreement) by providing them a copy of the audit results. The audit results will not be disclosed to subscribers and relying parties.

8.7 Self-Audits

Cybertrust conducts self-audits on a regular basis.

9. Other Business and Legal Matters

9.1 Fees

Fees shall be pursuant to the Cybertrust Device ID End User License Agreement to be executed by and between Cybertrust and the Subscriber Management Organization.

9.2 Financial Responsibility

Cybertrust shall maintain a sufficient financial foundation that is required for observing the subject matter set forth in this CPS and operating Certification Authorities.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Certification Authorities shall handle the following information as confidential information ("Confidential Information") among the information held by the Issuing Authority, the Registration Authority and the Device ID Support Desk:

(i) information relating to requests from the Subscriber Management Organization;

(ii) information set forth in "9.4.2 Information Treated as Private" of this CPS; and

(iii) information relating to the security of Certification Authorities.

9.3.2 Information not within the Scope of Confidential Information

Of the information held by the Issuing Authority, the Registration Authority and the Device ID Support Desk, Certification Authorities shall exclude the following information from the scope of Confidential Information:

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

(ii) issued certificates;

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

(iv) information which was disclosed and became public knowledge without any restriction of confidentiality from a party other than Certification Authorities; and

(v) information for which the Subscriber Management Organization approved in advance to the effect of being disclosed or provided to a third party.

With regard to information of subscribers and relying parties of the Device ID Certificate being managed by the Subscriber Management Organization other than the information listed above, the Subscriber Management Organization shall manage and handle such information under its own responsibility, and Certification Authorities shall not be responsible for managing such information, and will not treat such information as Confidential Information.

9.3.3 Responsibility to Protect Confidential Information

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

The handling of protection of personal information shall be set forth in "9.4 Privacy of Personal Information" of this CPS.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Of the information held by the Issuing Authority, the Registration Authority and the Device ID Support Desk, Certification Authorities shall handle information corresponding to "9.4.2 Information Treated as Private" of this CPS based on the Act on the Protection of Personal Information and the Amendment Act of the Act on the Protection of Personal Information, etc. with regard to matters other than the matters set forth in this CPS.

With regard to operations to be performed by Cybertrust among the operations to be performed by Certification Authorities, Cybertrust shall also observe the Privacy Policy published on the website (https://www.cybertrust.co.jp/corporate/privacy-policy.html) managed by Cybertrust.

9.4.2 Information Treated as Private

Issuing CA shall handle, as personal information, any information that is included in the issuance or revocation requests of the Device ID Certificate given by the Device ID Certificate Registration Authority to the Issuing Authority about a living individual which can identify the specific individual such as name, date of birth or other description by which the specific individual can be identified easily with referencing to other information).

9.4.3 Information not Deemed Private

Issuing CA shall not deem, as personal information, any information other than the information set forth in "9.4.2 Information Treated as Private" of this CPS.

9.4.4 Responsibility to Protect Private Information

The responsibility of protecting the personal information held by Issuing CA shall be as set forth in "9.4.1 Privacy Plan" of this CPS.

9.4.5 Notice and Consent to Use Private Information

Issuing CA shall deem that it has obtained the approval of the organization that made the request with regard to Isssuing CA performing the issuance/revocation operations of the Certificate scheduled in this CPS, implementing audits, and using personal information for operations that are otherwise required for providing the Service as a result of receiving the request for using the Service. Incidentally, Issuing CA shall not use the personal information for any purpose other than for providing the Service and performing the certification operations; save for the cases set forth in "9.4.6 Disclosure Pursuant to Judicial or Administrative Process" of this CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

When disclosure of personal information handled by Issuing CA is demanded in the course of judicial, administrative or other legal proceedings based on provisions of laws, Issuing CA may disclose such personal information.

9.4.7 Other Information Disclosure Circumstances

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

9.5 Intellectual Property Rights

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

(i) certificates issued by Certification Authorities and certificate revocation information;

(ii) this CPS and related documents;

(iii) public key and private key of Certification Authorities; and

(iv) hardware and software leased by Certification Authorities.

9.6 Representations and Warranties

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

9.6.1 IA Representations and Warranties

Cybertrust represents and warrants that it bears the following obligations upon performing operations of the Issuing Authorities as the Issuing Authorities which constitutes Certification Authorities:

(i) safely control the Certification Authority private key;

(ii) perform accurate certificate issuance and revocation based on instructions from the Registration Authority;

(iii) provide revocation information by issuing and publishing the 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

The Subscriber Management Organization operating the Device ID Certificate Registration Authority and Cybertrust operating the Network Equipment Dedicated Server Certificate Registration Authority represent and warrant that they bear the following obligations upon performing operations of the Registration Authorities as the Registration Authorities which constitutes Certification Authorities:

(i) observe this CPS and the Related Rules;

(ii) give accurate instructions to the Issuing Authority for issuing and revoking the Certificate;

(iii) properly notify a subscriber of the issuance of the Certificate, or properly distribute the issued Certificate to a subscriber; and

(iv) be responsible for any situations that arise as a result of any default of the Registration Authority's obligations prescribed in this paragraph.

9.6.3 Subscriber Management Organization Representations and Warranties

The Subscriber Management Organization represents and warrants that it bears the following obligations:

(i) observe this CPS and the Related Rules;

(ii) cause subscribers and relying parties under its management to observe this CPS and the Related Rules;

(iii) operate the Registration Authority;

(iv) accurately request the issuance or revocation of certificates to the Registration Authority;

(v) be responsible for any situations that arise as a result of any default of the Subscriber Management Organization's obligations prescribed in this paragraph; and

(vi) observe "4.9.1.3 Reason of Revocation by Subscriber Management Organization" of this CPS.

9.6.4 Subscriber Representations and Warranties

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

(i) observe this CPS and the Related Rules;

(ii) observe the certificate usage ("1.4.1 Appropriate Certificate Uses" of this CPS);

(iii) install the certificate only in a device approved by the Subscriber Management Organization and in a network equipment service that is being used or managed by the subscriber;

(iv) when installing the certificate in a device or a network equipment service, verify that the information included in the certificate is valid;

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

(vi) observe "4.9.1.3 Reason of Revocation by Subscriber" of this CPS; and

(vii) refrain from using an expired certificate or a revoked certificate.

9.6.5 Relying Party Representations and Warranties

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

(i) verify the certificate and configure the properly approved device or network equipment in a reliable manner in accordance with the instructions or rules of the Subscriber Management Organization, and observe this CPS and the Related Rules;

(ii) verify that the certificate is being used for the usage set forth in "1.4.1 Appropriate Certificate Uses" of this CPS;

(iii) verify the validity period and entries of the certificate issued by Certification Authorities;

(iv) verify the digital signature and verify the issuer of the certificate;

(v) verify whether the revocation based on CRL or OCSP has been registered; and

(vi) be responsible for any situations that arise as a result of any default of obligations prescribed in this paragraph.

9.6.6 Representations and Warranties of Other Participants

The Device ID Support Desk represents and warrants that it bears the following obligations:

(i) observe this CPS and the Related Rules;

(ii) accept inquiries ("1.5.2 Contact Person" of this CPS);

(iii) register and delete the Device ID Certificate Registration Authority;

(iv) manage the registration of the Device ID Certificate Registration Authority Operator Supervisor and the Registration Authority Operator;

(v) notify the Device ID Certificate Registration Authority or the Subscriber Management Organization upon acknowledging that correction is required;

(vi) perform counter services in the Network Equipment Dedicated Server Certificate Registration Authority; and

(vii) if the Certification Authority's private key is compromised, notify such fact to the relevant Subscriber Management Organization or publish such fact on the repository as needed.

9.7 Disclaimers of Warranties

Certification Authorities shall not be liable for any default based on this CPS regarding damages excluding direct damages arising in relation to the warranties set forth in "9.6.1 IA Representations and Warranties", "9.6.2 RA Representations and Warranties" and "9.6.6 Representations and Warranties of Other Participants" of this CPS.

Furthermore, even if any damage is directly suffered in relation to the foregoing warranties, such damage shall be handled in accordance with the Cybertrust Device ID End User License Agreement to be executed by and between Cybertrust and the Subscriber Management Organization, and Certification Authorities shall not be responsible in any way against the subscribers and relying parties.

9.8 Limitations of Liability

Certification Authorities shall not be liable in any way in the following cases in relation to the subject matter of "9.6.1 IA Representations and Warranties", "9.6.2 RA Representations and Warranties" and "9.6.6 Representations and Warranties of Other Participants" of this CPS:

(i) any damage that arises regardless of the Issuing Authority, the Registration Authority and the Device ID Support Desk observing this CPS and legal regulations;

(ii) any damage that arises due to fraud, unauthorized use or negligence that is not attributable to Certification Authorities;

(iii) any damage that arises due to the Subscriber Management Organization neglecting to perform its obligations borne based on the provisions of "9.6 Representations and Warranties" of this CPS;

(iv) damage that arises as a result of subscribers or relying parties neglecting to perform their respective obligations prescribed in "9.6 Representations and Warranties" of this CPS;

(v) damage that arises as a result of the key pair of the certificate issued by Certification Authorities being divulged or deciphered due to acts of a third party other than Certification Authorities;

(vi) damage that arises as a result of the certificate infringing upon the copyright, trade secret or any other intellectual property right of the Subscriber Management Organization, a subscriber, a relying party or a third party;

(vii) damage caused by the weakening of the cryptographic strength resulting from technological advances such as improvement in the encryption algorithm decoding technology, or by any other vulnerability; or

(viii) damage caused by any update or specification change of the software, OS, application or related services of the device that introduced a certificate.

The amount of damages to be borne by Cybertrust against the Subscriber Management Organization shall be pursuant to the Cybertrust Device ID End User License Agreement to be executed by and between Cybertrust and the Subscriber Management Organization.
Among the damages arising from any default or breach of this CPS or the Related Rules, Cybertrust shall not be liable for any data loss, indirect damages including lost profits, consequential damages and punitive damages to the extent permitted under the governing law set forth in "9.14 Governing Law" of this CPS.

9.9 Indemnities

The Subscriber Management Organization shall compensate any damage suffered by Certification Authorities due to claims made by a third party against Certification Authorities or lawsuits or other legal measures initiated or taken by a third party against Certification Authorities resulting from any of the following acts conducted by a subscriber or a relying party being managed by the Subscriber Management Organization, as well as become responsible for taking measures so that Certification Authorities will not suffer any more damage:

(i) unauthorized use, falsification, or misrepresentation during the use of the certificate;

(ii) breach of this CPS or the Related Rules; or

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

Certification Authorities are not the Subscriber Management Organization's, subscriber's or relying party's agent, trustee or any other representative.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

This CPS shall become invalid at the time that all Certification Authorities terminate their operations, excluding the cases prescribed in "9.10.3 Effect of Termination and Survival" of this CPS.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notifications and Communications with Participants

When Issuing CA is to notify subscribers independently, such as when sending a notification of issuance, such notice shall be deemed to have been made when it is sent out via email.

Notices from a subscriber shall be received by the Registration Authority that instructed the issuance of the Certificate to the subscriber, and Issuing CA and the Device ID Support Desk shall not directly receive notices from a subscriber of the Device ID Certificate and the Network Equipment Dedicated Server Certificate, unless expressly provided for herein.

Any notice concerning the request for using the Service or terminating the use of the Service shall be pursuant to the Cybertrust Device ID End User License Agreement to be executed by and between Cybertrust and the Subscriber Management Organization, and the handling of such notice is not prescribed in this CPS.

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS may be amended as needed based on instructions from the CTJ PA or the Supervisor of Certification Authorities. The CTJ PA shall approve the amendment of this CPS 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

In case of any amendments of this CPS, the CPS before amendment and the CPS after amendment are posted for a given period on the website so that the respective parties can verify the amended contents after the CTJ PA approves the amendment of this CPS. The amended CPS shall come into force at the time that is separately set forth by the CTJ PA. If the Subscriber Management Organization does not instruct the Registration Authority to revoke the certificate within fifteen (15) days after the effectuation thereof, it shall be deemed that the respective parties involved in the valid certificate have accepted the amended CPS.

9.12.3 Circumstances under Which OID Must Be Changed

Not applicable.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

Not applicable.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

Certification Authorities will not allow the assignment of operations of the Registration Authority to a third party.

The assignment of the Service by Cybertrust to a third party shall be pursuant to the Cybertrust Device ID End User License Agreement to be executed by and between Cybertrust and the Subscriber Management Organization.

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

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

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 validity period of that certificate.
Key Pair	A public key and a private key in public key cryptography. The two keys are unique in that one key cannot be derived from another key.
Key Length	A bit number that represents the key length which is also a factor in deciding the cryptographic strength.
Activation	To cause a system or device to be a usable state. Activation requires activation data, and specifically includes a PIN and pass phrase.
Compromise	A state where the confidentiality or completeness of information that is incidental to the private key and the private key is lost.
Public Key	One key of the key pair in public key cryptography that is notified to and used by the other party (communication partner, etc.).
Configuration Profile	XML file for iOS devices such as iPhones and iPads which includes the device security policy, VPN configuration information, Wi-Fi setting, APN setting, Exchange account setting, email setting, and certificates such as the Device ID Certificate of the corresponding device.
Common Name	Common Name (CN). Attribute Type in the Distinguished Name. Represents the individual name. Device Identifying Information (terminal asset management number, etc.) is indicated in the Device ID Certificated issued by Issuing CA.
Cybertrust Device ID End User License Agreement	Agreement to be executed by and between the Subscriber Management Organization and Cybertrust upon using the Service. This CPS constitutes a part of the Cybertrust Device ID End User License Agreement.
Revocation	Measure for invalidating a certificate even during the validity period of that certificate.
Self-signed Certificate	Self-signed Certificate. Certificate issued by the Certification Authority to certify itself. The party that issued the Certificate and the party to which the Certificate was issued, which are indicated on the Certificate, are the same.
Certificate	X.509 Public Key Certificate. Unless separately provided for herein, collectively referring to the Device ID Certificate and the Network Equipment Dedicated Server Certificate.
Certificate Revocation List	Abbreviated as “CRL” in this CPS. CRL is a list of revoked certificates. The Certification Authority publishes the CRL so that the subscribers and relying parties can verify the validity of the Certificate.

Organization Unit Name	Organization Unit Name (OU). Attribute Type in the Distinguished Name. Generally represents the name of the business division, and multiple names may be designated. A name capable of uniquely categorizing the Subscriber Management Organization is indicated as one OU in the Device ID Certificate issued by Issuing CA. Moreover, up to two OUs can be designated, and the names of the business divisions, etc. are indicated.
Organization Name	Organization Name (O). Attribute Type in the Distinguished Name. Generally represents the name of the organization. A name capable of uniquely categorizing the Subscriber Management Organization is indicated on the Device ID Certificate issued by Issuing CA.
Device	Device or terminal connected to a network such as a PC, smartphone or other business terminals.
Electronic Signature	Electronic data for unmistakably certifying the person. Used to mean a digital signature in this CPS. Specifically, electronic data that is encrypted with a private key against a hash value of the data to be signed. A digital signature can be verified by comparing the value decrypted with the public key and the hash value of the original data.
Certification Operations	Series of operations that are performed during the life cycle controls of the Certificate. 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.
Private Key	One key of the key pair in public key cryptography that is kept private from others.
Policy	Policy to be followed upon operating Certification Authorities, or used as a term referring to the guidelines on how the Certificate will be used. Prescribed as the Certification Practice Statement “CPS” in the case of the former and prescribed as the Certificate Policy “CP” in the case of the latter, but there are cases where the CPS is formulated in a manner of including the CP without specifically categorizing the CP. This CPS includes the CP.
Escrow	As used herein, the term “escrow” refers to the processing of registering and storing a private key or a public key with a third party.
Repository	A website or system for posting public information such as this CPS and CRL.
CP	Certificate Policy. A document which prescribes the purpose of use, applicable scope and other guidelines of the Certificate.
CPS	Certification Practice Statement. A document which prescribes the responsibilities and obligations, operating policy, operating procedures and other matters of Certification Authorities.
CRL	Certificate Revocation List.
Distinguished Name	An identifier set forth in the X.500 recommendation formulated by ITU-T. Configured from attribute information such as a common name, organization name, organizational unit name, and country name.

FIPS 140 Level 4	FIPS (Federal Information Processing Standards Publication 140) is a U.S. federal standard that prescribes the specifications of security requirements in a cryptographic module. With this standard, the security requirements are classified as the levels of 1 (lowest) to 4 (highest).
IETF PKIX Working Group	Internet Engineering Task Force (IETF) is an organization that standardizes technologies used for the internet, and the PKIX Working Group of IETF set forth RFC3647.
ITU-T	Telecommunications Standardization Sector of the International Telecommunication Union.
OCSP	Online Certificate Status Protocol. A communication protocol for verifying certificate revocation information. Certification Authorities is operating an OCSP server, in addition to publicly disclosing CRL, so that a relying party can verify the validity of a certificate.
Network Equipment	Network equipment or equipment on a network such as a server equipment, and in particular refers to equipment to be used in combination with a supplicant equipped in iOS, Android and Windows OS as a standard feature upon using the Device ID Certificate.
MAC Address	ID number unique to each Ethernet network interface. A MAC address is uniquely assigned globally to each physical interface, and data transfer between cards is performed based thereon. Devices can be identified by leveraging the uniqueness thereof.
PKI	Public Key Infrastructure. Collective designation of the architecture, operation, procedures and the like using public key cryptography.
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.
X.500	International standard of distribution directory services to be provided on a network standardized by ITU-T.
X.509	International standard of the Certificate standardized by ITU-T.

Appendix B: Certificate Profile

Self-signed Certificate

(Basic Certificate Fields)

Version		**Value**
Version	Version of the encoded certificate Type: INTEGER Value: 2	 2 (Ver.3)
serialNumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique Integer	 *Serial Number
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 Value: One of the values on the right	 CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2t: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3s: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3is: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3sp: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3t: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3h: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3isr: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3hedu: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3hedu: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3m: 1.2.840.113549.1.1.11(SHA256withRSA) G4pr<xxx> 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	Parameters of cryptographic algorithm Type: NULL Value:	 NULL
Issuer		**Value**
CountryName	Country name attribute of certificate issuer	
Type	Object ID for the country name Type: OID Value: 2 5 4 6	 2.5.4.6
Value	Value of country name Type: PrintableString Value: JP	 JP
OrganizationName	Organization name attribute of certificate issuer	
Type	Object ID for organization name Type: OID	

	Value: 2 5 4 10	2.5.4.10
Value	Value of organization name Type: PrintableString	
	Value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	Common name attribute of certificate issuer	
Type	Object ID for common name Type: OID	
	Value: 2 5 4 3	2.5.4.3
Value	Value of common name Type: PrintableString	
	Value: One of the Certification Authorities on the right	Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G2t Cybertrust DeviceiD Public CA G3 Cybertrust DeviceiD Public CA G3s Cybertrust DeviceiD Public CA G3k Cybertrust DeviceiD Public CA G3is Cybertrust DeviceiD Public CA G3sp Cybertrust DeviceiD Public CA G3t Cybertrust DeviceiD Public CA G3h Cybertrust DeviceiD Public CA G3isr Cybertrust DeviceiD Education CA G3h Cybertrust DeviceiD Public CA G3m Cybertrust DeviceiD Private CA G4pr<xxx> Cybertrust DeviceiD Premium CA G4pr<xxx> Cybertrust DeviceiD Premium Root G4pr<xxx>
Validity		**Value**
Validity		The all Certification Authorities has following value 15 Years + 1 Month
notBefore	The date on which the certificate validity period begins Type: UTCTime or GeneralizedTime	Following value depending on the Certification Authority
	Value: yy (2 digit or 4 digit) mmddhhmmssZ	CA G2: 131016025113Z CA G2s: 131016110203Z CA G2k: 131017021450Z CA G2is: 140320051900Z CA G2sp: 141205021856Z CA G2t: 151127020112Z CA G3: 150527014541Z CA G3s: 150527022814Z CA G3k: 150420054150Z CA G3is: 150707014526Z CA G3sp: 150707022009Z CA G3t: 151127025137Z CA G3h: 161201024543Z CA G3isr: 180206045700Z CA G3hedu: 200722064824Z CA G3m: 211201081956Z G4pr<xxx>: depends on each CA
notAfter	The date on which the certificate validity period ends Type: UTCTime or GeneralizedTime	Following value depending on the Certification Authority
	Value: yy (2 digit or 4 digit) mmddhhmmssZ	CA G2: 281116025113Z CA G2s: 281116110203Z CA G2k: 281117021450Z CA G2is: 290420051900Z CA G2sp: 300105021856Z CA G2t: 301227020112Z CA G3: 300627014541Z CA G3s: 300627022814Z CA G3k: 300520054150Z CA G3is: 300807014526Z CA G3sp: 300807022009Z CA G3t: 301227025137Z CA G3h: 320101024543Z CA G3isr: 330306045700Z CA G3hedu: 350822064824Z

		CA G3m: 370101081956Z CA G4pr<xxx>: depends on each CA
Subject		**Value**
CountryName	Country name attribute of certificate issuer	
Type	Object ID for the country name Type: OID Value: 2 5 4 6	 2.5.4.6
Value	Value of country name Type: PrintableString Value: JP	 JP
OrganizationName	Organization name attribute of certificate issuer	
Type	Object ID for organization name Type: OID Value: 2 5 4 10	 2.5.4.10
Value	Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd.	 Cybertrust Japan Co., Ltd.
CommonName	Common name attribute of certificate issuer	
Type	Object ID for common name Type: OID Value: 2 5 4 3	 2.5.4.3
Value	Object ID for common name Type: PrintableString Value: One of the Certification Authorities on the right; provided, however, that this shall be the same value as the Issuer name	 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G2t Cybertrust DeviceiD Public CA G3 Cybertrust DeviceiD Public CA G3s Cybertrust DeviceiD Public CA G3k Cybertrust DeviceiD Public CA G3is Cybertrust DeviceiD Public CA G3sp Cybertrust DeviceiD Public CA G3t Cybertrust DeviceiD Public CA G3h Cybertrust DeviceiD Public CA G3isr Cybertrust DeviceiD Education CA G3h Cybertrust DeviceiD Public CA G3m Cybertrust DeviceiD Private CA G4pr<xxx> Cybertrust DeviceiD Premium CA G4pr<xxx> Cybertrust DeviceiD Premium Root G4rt<xxx>
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 (RSA PUBLIC KEY) Type: OID Value: 1 2 840 113549 1 1 1	 1.2.840.113549.1.1.1
Parameters	Parameters of cryptographic algorithm Type: NULL Value:	 NULL
subjectPublicKey	Value of public key Type: BIT STRING Value: Public Key Value	 *2048Bits,3072Bits or 4096Bits

(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 Value: True (CA)	 TRUE
subjectKeyIdentifier (extnId:== 2 5 29 14, critical:== FALSE)		**Value**
SubjectKeyIdentifier	Subject Key Identifier	
keyIdentifier	The identifier for public key	

	Type: OCTET STRING Value: Hash value of the Issuer's subjectPublicKey	Following value depending on the Certification Authority CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G2t: 43:AD:48:61:61:82:22:3B:AE:04: C4:1B:8A:B7:A4:72:0B:D1:28:9B CA G3: ED:16:DC:25:12:A8:94:61:7D:8B: 1F:74:C9:D1:E4:D5:F8:08:7C:C0 CA G3s: 01:A1:CF:28:36:47:39:A3:4C:2A: 41:F5:99:84:E4:22:72:28:05:A0 CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC CA G3is: 38:9B:03:06:BA:F7:76:30:ED:16: AC:1A:28:22:33:F2:85:0C:73:54 CA G3sp: B8:79:07:36:4C:FD:24:CD:B3:F6: 0B:F0:07:61:BF:83:12:DC:1A:04 CA G3t: C9:73:E2:3F:C6:0E:72:31:E1:77: 4A:2E:C7:22:7D:C4:FD:24:05:C7 CA G3h: BD:20:46:2C:8C:68:DD:B4:66:28: 31:F2:72:B2:59:2E:32:19:B2:43 CA G3isr: B0:4C:A9:A0:09:F7:0C:C1:94:7C: C0:9D:5D:86:12:99:B8:FC:0E:73 CA G3hedu: 62:38:53:2A:5E:D5:E3:4C:6D:34: 4E:59:E3:47:8E:30:29:E0:BB:D6 CA G3m: A8:B3:38:82:66:EF:14:91:03:8F: 02:30:45:33:56:DD:7A:3F:D8:12 G4pr<xxx>: depends on each CA
keyUsage (extnId:== 2 5 29 15, critical:== TRUE)		**Value**
KeyUsage	Key Usage Type: BIT STRING Value: 00000110 (CertificateSigning, CRLSigning)	00000110

Certification Authority Certificate

(Basic Certificate Fields)

Version		**Value**
Version	Version of the encoded certificate Type: INTEGER Value: 2	 2 (Ver.3)
serialNumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique Integer	 *Serial Number
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 Value:	 1.2.840.113549.1.1.11(SHA256withRSA) NULL
Issuer		**Value**
CountryName Type Value OrganizationName Type Value CommonName Type Value	Country name attribute of certificate issuer Object ID for the country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization name attribute of certificate issuer Object ID for organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name attribute of certificate issuer Object ID for common name Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust DeviceiD Premium Root G4pr<xxx>
Validity		**Value**
Validity notBefore notAfter 	 The date on which the certificate validity period begins Type: UTCTime or GeneralizedTime Value: yy (2 digit or 4 digit) mmddhhmmssZ The date on which the certificate validity period ends Type: UTCTime or GeneralizedTime Value: yy (2 digit or 4 digit) mmddhhmmssZ	15 Years + 1 Month CA G4pr<xxx>: depends on each CA CA G4pr<xxx>: depends on each CA
Subject		**Value**
CountryName Type Value OrganizationName Type Value	Country name attribute of certificate issuer Object ID for the country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization name attribute of certificate issuer Object ID for organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd.	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co., Ltd.

CommonName Type Value 	Common name attribute of certificate issuer Object ID for common name Type: OID Value: 2 5 4 3 Object ID for common name Type: PrintableString Value: One of the Certification Authorities on the right.	 2.5.4.3 Cybertrust DeviceiD Private CA G4pr<xxx> Cybertrust DeviceiD Premium CA G4pr<xxx>
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo AlgorithmIdentifier Algorithm Parameters subjectPublicKey 	Subject's public key information The identifier for cryptographic algorithm (public key cryptosystem and hash) Object ID for the cryptographic algorithm (RSA PUBLIC KEY) Type: OID Value: 1 2 840 113549 1 1 1 Parameters of cryptographic algorithm Type: NULL Value: Value of public key Type: BIT STRING Value: Public Key Value	 1.2.840.113549.1.1.1 NULL *2048Bits,3072Bits or 4096Bits

(Certificate Extensions)

basicConstraints (extnId:== 2 5 29 19, critical:== TRUE)		**Value**
BasicConstraints cA	Basic Constraints The flag to determine whether the supplied certificate is associated with a CA or an end entity Type: Boolean Value: True (CA)	 TRUE
subjectKeyIdentifier (extnId:== 2 5 29 14, critical:== FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Subject Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of the Issuer's subjectPublicKey	 CA G4pr<xxx>:depends on each CA
keyUsage (extnId:== 2 5 29 15, critical:== TRUE)		**Value**
KeyUsage	Key Usage Type: BIT STRING Value: 00000110 (CertificateSigning, CRLSigning)	 00000110
authorityKeyIdentifier (extnId:== 2 5 29 35, critical:== FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Authority Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of Certification Authority's subjectPublicKey	 depends on Root CA
cRLDistributionPoints (extnId:== 2 5 29 31, critical:== FALSE)		**Value**
cRLDistributionPoints DistributionPoint fullName	CRL Distribution Point CRL Distribution Point URI of CRL Distribution Point Type: OCTET STRING Value: http URI	 CAG4pr<xxx>: http://crl.deviceid.ne.jp/deviceid/g4rtpr<xxx>.crl
authorityInfoAccess (extnId:== 1 3 6 1 5 5 7 1 1, critical:== FALSE)		**Value**
Authority Information Access Access Method Access Location	Authority Information Access Access method Type: OID Value: 1 3 6 1 5 5 7 48 1 Access location Type: IA5String Value: URL of OCSP	*OCSP if provided 1.3.6.1.5.5.7.48.1 (OCSP) http://ocsp-rtpr.deviceid.ne.jp/deviceid

Device ID Certificate

Shaded areas can be set up based on application by the Subscriber Management Organization

(Basic Certificate Fields)

Version		**Value**
Version	Version of the encoded certificate Type: INTEGER Value: 2	 2 (Ver.3)
serialNumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique Integer	 *Serial Number
Signature		**Value**
AlgorithmIdentifier	The identifier for cryptographic algorithm (public key cryptosystem and hash)	
Algorithm	Object ID for the cryptographic algorithm Type: OID Value: One of the values on the right	 CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2t: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3s: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3is: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3sp: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3t: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3h: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3isr: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3hedu: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3m: 1.2.840.113549.1.1.11(SHA256withRSA) CA G4pr<xxx>: 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	Parameters of cryptographic algorithm Type: NULL Value:	 NULL
Issuer		**Value**
CountryName	Country-name attribute of certificate issuer	
Type	Object ID for the country name Type: OID Value: 2 5 4 6	 2.5.4.6
Value	Value of country name Type: PrintableString Value: JP	 JP
OrganizationName	Organization name attribute of certificate issuer	
Type	Object ID for organization name Type: OID Value: 2 5 4 10	 2.5.4.10
Value	Value of organization name Type: PrintableString	

	Value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	Common name attribute of certificate issuer	
Type	Object ID for common name	
	Type: OID	
	Value: 2 5 4 3	2.5.4.3
Value	Value of common name	
	Type: PrintableString	
	Value: One of the Certification Authorities on the right to issue the Device ID Certificate	Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G2t Cybertrust DeviceiD Public CA G3 Cybertrust DeviceiD Public CA G3s Cybertrust DeviceiD Public CA G3k Cybertrust DeviceiD Public CA G3is Cybertrust DeviceiD Public CA G3sp Cybertrust DeviceiD Public CA G3t Cybertrust DeviceiD Public CA G3h Cybertrust DeviceiD Public CA G3isr Cybertrust DeviceiD Education CA G3h Cybertrust DeviceiD Public CA G3m Cybertrust DeviceiD Private CA G4pr<xxx> Cybertrust DeviceiD Premium CA G4pr<xxx>
Validity		**Value**
Validity	Validity period of certificate	
notBefore	The date on which the certificate validity period begins	
	Type: UTCTime or GeneralizedTime	
	Value: yy (2 digit or 4 digit) mmddhhmmssZ	Ex: 090401000000Z
notAfter	The date on which the certificate validity period ends	
	Type: UTCTime or GeneralizedTime	
	Value: yy (2 digit or 4 digit) mmddhhmmssZ	Ex: 140501000000Z
Subject		**Value**
CountryName	Country name attribute of certificate subject	
Type	Object ID for the country name	
	Type: OID	
	Value: 2 5 4 6	2.5.4.6
Value	Value of country name	
	Type: PrintableString	
	Value: JP	JP
OrganizationName	Organization name attribute of certificate subject	
Type	Object ID for organization name	
	Type: OID	
	Value: 2 5 4 10	2.5.4.10
Value	Value of organization name	
	Type: PrintableString or UTF8String	*To be changed depending on the character value
	Value: <<Name of Customer's Company + Corporation identifier>>	*Corporation identifier is uniquely prescribed by the Device ID Support Desk
OrganizationalUnitName(1)	Organizational unit name attribute of certificate subject	
Type	Object ID for the organizational unit name	
	Type: OID	
	Value: 2 5 4 11	2.5.4.11
Value	Value of organizational unit name	
	Type: PrintableString or UTF8String	*To be changed depending on the character value
	Value: RA operated by <<Name of Customer's Company + Corporation identifier>>	Corporation identifier is uniquely prescribed by the Device ID Support Desk
OrganizationalUnitName(2, 3)	Organizational unit name attribute of certificate subject	*Optional item (up to two terms may be used)
Type	Object ID for the organizational unit name	
	Type: OID	
	Value: 2 5 4 11	2.5.4.11
Value	Value of organizational unit name	
	Type: PrintableString or UTF8String	*To be changed depending on the character value
	Value: <<DepartmentName>>	

CommonName Type Value	Common name attribute of certificate subject Object ID for common name Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString or UTF8String Value: <<Device Identifying Information>>	 2.5.4.3 *To be changed depending on the character value Terminal asset management number, etc.
subjectPublicKeyInfo		**Value**
SubjectPublicKeyInfo AlgorithmIdentifier Algorithm parameters subjectPublicKey	Subject's public key information The identifier for cryptographic algorithm (public key cryptosystem and hash) Object ID for the cryptographic algorithm (RSA PUBLIC KEY) Type: OID Value: 1 2 840 113549 1 1 1 Parameters of cryptographic algorithm Type: NULL Value: Public Key Value Type: BIT STRING Value: Public Key Value	 1.2.840.113549.1.1.1 NULL *Key Length is 2048 bits,3072bits or 4096bits (1024 bits may be permitted in certain cases)

(Certificate Extensions)

authorityKeyIdentifier (extnId:== 2 5 29 35, critical:== FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Authority Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of Certification Authority's subjectPublicKey	 Following value depending on the Certification Authority CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G2t: 43:AD:48:61:61:82:22:3B:AE:04: C4:1B:8A:B7:A4:72:0B:D1:28:9B CA G3: ED:16:DC:25:12:A8:94:61:7D:8B: 1F:74:C9:D1:E4:D5:F8:08:7C:C0 CA G3s: 01:A1:CF:28:36:47:39:A3:4C:2A: 41:F5:99:84:E4:22:72:28:05:A0 CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC CA G3is: 38:9B:03:06:BA:F7:76:30:ED:16: AC:1A:28:22:33:F2:85:0C:73:54 CA G3sp: B8:79:07:36:4C:FD:24:CD:B3:F6: 0B:F0:07:61:BF:83:12:DC:1A:04 CA G3t: C9:73:E2:3F:C6:0E:72:31:E1:77: 4A:2E:C7:22:7D:C4:FD:24:05:C7 CA G3h: BD:20:46:2C:8C:68:DD:B4:66:28: 31:F2:72:B2:59:2E:32:19:B2:43 CA G3isr:

		B0:4C:A9:A0:09:F7:0C:C1:94:7C: C0:9D:5D:86:12:99:B8:FC:0E:73 CA G3hedu: 62:38:53:2A:5E:D5:E3:4C:6D:34: 4E:59:E3:47:8E:30:29:E0:BB:D6 CA G3m: A8:B3:38:82:66:EF:14:91:03:8F: 02:30:45:33:56:DD:7A:3F:D8:12 CA G4pr<xxx>: depends on each CA
authorityCertIssuer	Type: GeneralNames Value: Value of Certification Authority's subject	Following value depending on the Certification Authority CA G2: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G2 CA G2s: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G2s CA G2k: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G2k CA G2is: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G2is CA G2sp: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G2sp CA G2t: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G2t CA G3: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3 CA G3s: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3s CA G3k: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3k CA G3is: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3is CA G3sp: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3sp CA G3t: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3t CA G3h: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3h CA G3isr: c=JP,o=Cybertrust Japan Co., Ltd., cn=Cybertrust DeviceiD Public CA G3isr CA G3hedu: c=JP,o=Cybertrust Japan Co., Ltd., cn= Cybertrust DeviceiD Education CA G3h CA G3m: c=JP,o=Cybertrust Japan Co., Ltd., cn= Cybertrust DeviceiD Public CA G3m CA G4dp<xxx>: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Private CA G4pr<xxx> CA G4dp<xxx>: c=JP,o=Cybertrust Japan Co.,Ltd., cn=Cybertrust DeviceiD Premium CA G4pr<xxx>
authorityCertSerialNumber	Type: INTEGER Value: serialNumber value of Certification Authority's Certificate	*Serial Number of Issuer's Certificate (differs depending on the Certification Authority)
subjectKeyIdentifier (extnId:== 2 5 29 14, critical:== FALSE)		**Value**

SubjectKeyIdentifier keyIdentifier	Information of Subject Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of the Issued Party's subjectPublicKey	 *Hash value of the Issued Party's subjectPublicKey
keyUsage (extnId:== 2 5 29 15, critical:== FALSE)		**Value**
KeyUsage	Key Usage Type: BIT STRING Value: 101000000 (digitalSignature,keyEncipherment)	 101000000
cRLDistributionPoints (extnId:== 2 5 29 31, critical:== FALSE)		**Value**
cRLDistributionPoints DistributionPoint fullName	CRL Distribution Point CRL Distribution Point URI of CRL Distribution Point Type: OCTET STRING Value: http URI	 Following value depending on the Certification Authority CA G2: http://crl.deviceid.ne.jp/deviceid/g2.crl CA G2s: http://crl.deviceid.ne.jp/deviceid/g2s.crl CA G2k: http://crl.deviceid.ne.jp/deviceid/g2k.crl CA G2is: http://crl.deviceid.ne.jp/deviceid/g2is.crl CA G2sp: http://crl.deviceid.ne.jp/deviceid/g2sp.crl CA G2t: http://crl.deviceid.ne.jp/deviceid/g2t.crl CA G3: http://crl.deviceid.ne.jp/deviceid/g3.crl CA G3s: http://crl.deviceid.ne.jp/deviceid/g3s.crl CA G3k: http://crl.deviceid.ne.jp/deviceid/g3k.crl CA G3is: http://crl.deviceid.ne.jp/deviceid/g3is.crl CA G3sp: http://crl.deviceid.ne.jp/deviceid/g3sp.crl CA G3t: http://crl.deviceid.ne.jp/deviceid/g3t.crl CA G3h: http://crl.deviceid.ne.jp/deviceid/g3h.crl CA G3isr: http://crl.deviceid.ne.jp/deviceid/g3isr.crl CA G3hedu: http://crl.deviceid.ne.jp/deviceid/g3hedu.crl CA G3m: http://crl.deviceid.ne.jp/deviceid/g3m.crl CA G4pr<xxx>: http://crl.deviceid.ne.jp/deviceid/g4pr<xxx>
subjectAltName (extnId:== 2 5 29 17, critical:== FALSE)		**Value**
subjectAltName dNSName otherName Type Value	Subject Alternative Name DNSName Type: IA5String Value: Full computer name Object ID for the UPN Type: OID Value: 1 3 6 1 4 1 311 20 2 3 UPN Type: UTF8String Value: User principal name	 (Option when using ActiveDirectory) (UPN option) 1.3.6.1.4.1.311.20.2.3
extendedKeyUsage (extnId:== 2 5 29 37, critical:== FALSE)		**Value**
extendedKeyUsage KeyPurposeId clientAuth	Extended Key Usage The purpose of the key contained in the certificate clientAuth Type: OID Value: 1 3 6 1 5 5 7 3 2	 1.3.6.1.5.5.7.3.2 (clientAuth)
authorityInfoAccess (extnId:== 1 3 6 1 5 5 7 1 1, critical:== FALSE)		**Value**
Authority Information Access	Authority Information Access	*Limited to the following Certification Authorities: CA G3, CA G3s, CA G3k, CA

		G3is, CA G3sp, CA G3t, CA G3h, CA G3isr, CA G3hedu,CA G3m, CA G4pr<xxx>
Access Method	Access method Type: OID Value: 1 3 6 1 5 5 7 48 1	1.3.6.1.5.5.7.48.1 (OCSP)
Access Location	Access location Type: IA5String Value: URL of OCSP	http://ocsp.deviceid.ne.jp/deviceid CA G4pr<xxx> : http://ocsp-pr.deviceid.ne.jp/deviceid

Network Equipment Dedicated Server Certificate

(Basic Certificate Fields)

Version		**Value**
Version	Version of the encoded certificate Type: INTEGER Value: 2	 2 (Ver.3)
serialNumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique Integer	 *Serial Number
Signature		**Value**
AlgorithmIdentifier	The identifier for cryptographic algorithm (public key cryptosystem and hash)	
Algorithm	Object ID for the cryptographic algorithm Type: OID Value: One of the values on the right	 CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2t: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3s: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3is: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3sp: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3t: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3h: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3isr: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3hedu: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3m: 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	Parameters of cryptographic algorithm Type: NULL Value:	 NULL
Issuer		**Value**
CountryName	Country-name attribute of certificate issuer	
Type	Object ID for the country name Type: OID Value: 2 5 4 6	 2.5.4.6
Value	Value of country name Type: PrintableString Value: JP	 JP
OrganizationName	Organization name attribute of certificate issuer	
Type	Object ID for organization name Type: OID Value: 2 5 4 10	 2.5.4.10
Value	Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd.	 Cybertrust Japan Co., Ltd.
CommonName	Common name attribute of certificate issuer	
Type	Object ID for common name Type: OID Value: 2 5 4 3	 2.5.4.3
Value	Value of common name Type: PrintableString Value: One of the Certification Authorities on the right to issue the Network	 Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s

	Equipment Dedicated Server Certificate	Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G2t Cybertrust DeviceiD Public CA G3 Cybertrust DeviceiD Public CA G3s Cybertrust DeviceiD Public CA G3k Cybertrust DeviceiD Public CA G3is Cybertrust DeviceiD Public CA G3sp Cybertrust DeviceiD Public CA G3t Cybertrust DeviceiD Public CA G3h Cybertrust DeviceiD Public CA G3isr Cybertrust DeviceiD Education CA G3h Cybertrust DeviceiD Public CA G3m
Validity		**Value**
Validity	Validity period of certificate	5 Years + within grace period (2 Months); provided, however, that this shall be 2 Years + with 2 months for Certificates issued by a Certification Authority in which the signature algorithm is compliant with SHA256withRSA from September 12, 2019 onward
notBefore	The date on which the certificate validity period begins Type: UTCTime or GeneralizedTime Value: yy (2 digit or 4 digit) mmddhhmmssZ	 Ex: 090401000000Z
notAfter	The date on which the certificate validity period ends Type: UTCTime or GeneralizedTime Value: yy (2 digit or 4 digit) mmddhhmmssZ	 Ex: 140601000000Z
Subject		**Value**
CountryName	Country name attribute of certificate subject	
Type	Object ID for the country name Type: OID Value: 2 5 4 6	 2.5.4.6
Value	Value of country name Type: PrintableString Value: JP	 JP
StateOrProvinceName	State or Province name attribute of certificate subject	*Only when required
Type	Object ID for the state or province name Type: OID Value: 2 5 4 8	 2.5.4.8
Value	Value of state or province name Type: PrintableString Value: <<State or province name>>	
LocalityName	Locality name attribute of certificate subject	*Only when required
Type	Object ID for the locality name Type: OID Value: 2 5 4 7	 2.5.4.7
Value	Value of locality name Type: PrintableString Value: <<Locality name>>	
OrganizationName	Organization name attribute of certificate subject	
Type	Object ID for organization name Type: OID Value: 2 5 4 10	 2.5.4.10
Value	Value of organization name Type: PrintableString or UTF8String Value: <<Name of Customer's Company + Corporation identifier>>	 *To be changed depending on the character value *Corporation identifier is uniquely prescribed by the Device ID Support Desk
OrganizationalUnitName(1,2)	Organizational unit name attribute of certificate subject	*Optional item (up to two terms may be used)
Type	Object ID for the organizational unit name Type: OID Value: 2 5 4 11	 2.5.4.11
Value	Value of organizational unit name Type: PrintableString or UTF8String Value: <<DepartmentName>>	 *To be changed depending on the character value
CommonName	Common name attribute of certificate subject	FQDN of Network Equipment
Type	Object ID for common name	

Value	Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString Value: <<Proper name>>	2.5.4.3 FQDN of Network Equipment
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 (RSA PUBLIC KEY) Type: OID Value: 1 2 840 113549 1 1 1	 1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm Type: NULL Value:	 NULL
subjectPublicKey	Public Key Value Type: BIT STRING Value: Public Key Value	 *Key Length is 2048 bits,3072bits or 4096bits (1024 bits may be permitted in certain cases)

(Certificate Extensions)

authorityKeyIdentifier (extnId:== 2 5 29 35, critical:== FALSE)		**Value**
AuthorityKeyIdentifier	Authority Key Identifier	
keyIdentifier	The identifier for public key Type: OCTET STRING Value: Hash value of Certification Authority's subjectPublicKey	 Following value depending on the Certification Authority CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G2t: 43:AD:48:61:61:82:22:3B:AE:04: C4:1B:8A:B7:A4:72:0B:D1:28:9B CA G3: ED:16:DC:25:12:A8:94:61:7D:8B: 1F:74:C9:D1:E4:D5:F8:08:7C:C0 CA G3s: 01:A1:CF:28:36:47:39:A3:4C:2A: 41:F5:99:84:E4:22:72:28:05:A0 CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC CA G3is: 38:9B:03:06:BA:F7:76:30:ED:16: AC:1A:28:22:33:F2:85:0C:73:54 CA G3sp: B8:79:07:36:4C:FD:24:CD:B3:F6: 0B:F0:07:61:BF:83:12:DC:1A:04 CA G3t: C9:73:E2:3F:C6:0E:72:31:E1:77: 4A:2E:C7:22:7D:C4:FD:24:05:C7 CA G3h: BD:20:46:2C:8C:68:DD:B4:66:28: 31:F2:72:B2:59:2E:32:19:B2:43 CA G3isr: B0:4C:A9:A0:09:F7:0C:C1:94:7C: C0:9D:5D:86:12:99:B8:FC:0E:73 CA G3hedu:

		62:38:53:2A:5E:D5:E3:4C:6D:34: 4E:59:E3:47:8E:30:29:E0:BB:D6 CA G3m: A8:B3:38:82:66:EF:14:91:03:8F: 02:30:45:33:56:DD:7A:3F:D8:12
subjectKeyIdentifier (extnId:== 2 5 29 14, critical:== FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Subject Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of the Issued Party's subjectPublicKey	 *Hash value of the Issued Party's subjectPublicKey
keyUsage (extnId:== 2 5 29 15, critical:== FALSE)		**Value**
KeyUsage	Key Usage Type: BIT STRING Value: 101000000 (digitalSignature,keyEncipherment)	 101000000
extendedKeyUsage (extnId:== 2.5.29.37, critical:== FALSE)		**Value**
extendedKeyUsage	Extended Key Usage Type: OID Value: 1.3.6.1.5.5.7.3.1 Type: OID Value: 1.3.6.1.5.5.7.3.2	 1.3.6.1.5.5.7.3.1(serverAuth) 1.3.6.1.5.5.7.3.2(clientAuth)
cRLDistributionPoints (extnId:== 2 5 29 31, critical:== FALSE)		**Value**
cRLDistributionPoints DistributionPoint fullName	CRL Distribution Point CRL Distribution Point URI of CRL Distribution Point Type: OCTET STRING Value: http URI	 Following value depending on the Certification Authority CA G2: http://crl.deviceid.ne.jp/deviceid/g2.crl CA G2s: http://crl.deviceid.ne.jp/deviceid/g2s.crl CA G2k: http://crl.deviceid.ne.jp/deviceid/g2k.crl CA G2is: http://crl.deviceid.ne.jp/deviceid/g2is.crl CA G2sp: http://crl.deviceid.ne.jp/deviceid/g2sp.crl CA G2t: http://crl.deviceid.ne.jp/deviceid/g2t.crl CA G3: http://crl.deviceid.ne.jp/deviceid/g3.crl CA G3s: http://crl.deviceid.ne.jp/deviceid/g3s.crl CA G3k: http://crl.deviceid.ne.jp/deviceid/g3k.crl CA G3is: http://crl.deviceid.ne.jp/deviceid/g3is.crl CA G3sp: http://crl.deviceid.ne.jp/deviceid/g3sp.crl CA G3t: http://crl.deviceid.ne.jp/deviceid/g3t.crl CA G3h: http://crl.deviceid.ne.jp/deviceid/g3h.crl CA G3isr: http://crl.deviceid.ne.jp/deviceid/g3isr.crl CA G3hedu: http://crl.deviceid.ne.jp/deviceid/g3hedu.crl CA G3m: http://crl.deviceid.ne.jp/deviceid/g3m.crl
subjectAltName (extnId:== 2 5 29 17, critical:== FALSE)		**Value**
subjectAltName dNSName iPAddress	Subject Alternative Name Full computer name Type: IA5String Value: Full computer name iPAddress Type: OCTET STRING Value: <<Owner's proper name>>	(Option when using ActiveDirectory) *Full computer name *IP address of server to perform SSL/TLS communication

OCSP Server Certificate (if provided)

(Basic Certificate Fields)

Version		**Value**
Version	Version of the encoded certificate Type: INTEGER Value: 2	 2 (Ver.3)
Serialnumber		**Value**
CertificateSerialNumber	Serial number of certificate Type: INTEGER Value: Unique Integer	 *Serial Number(Unique Integer)
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 Value: Type: NULL Value:	 1.2.840.113549.1.1.11(SHA256withRSA) NULL
Issuer		**Value**
CountryName Type Value OrganizationName Type Value CommonName Type Value	Country-name attribute of certificate issuer Object ID for the country name Type: OID Value: 2 5 4 6 Value of country name Type: PrintableString Value: JP Organization name attribute of certificate issuer Object ID for organization name Type: OID Value: 2 5 4 10 Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd. Common name attribute of certificate issuer Object ID for common name Type: OID Value: 2 5 4 3 Value of common name Type: PrintableString Value: One of the Certification Authorities on the right to issue the OCSP Server Certificate	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust DeviceiD Public CA G3 Cybertrust DeviceiD Public CA G3s Cybertrust DeviceiD Public CA G3k Cybertrust DeviceiD Public CA G3is Cybertrust DeviceiD Public CA G3sp Cybertrust DeviceiD Public CA G3t Cybertrust DeviceiD Public CA G3h Cybertrust DeviceiD Public CA G3isr Cybertrust DeviceiD Education CA G3h Cybertrust DeviceiD Public CA G3m Cybertrust DeviceiD Private CA G4pr<xxx> Cybertrust DeviceiD Premium CA G4pr<xxx> Cybertrust DeviceiD Premium Root G4pr<xxx>
Validity		**Value**
Validity notBefore notAfter 	Validity period of certificate The date on which the certificate validity period begins Type: UTCTime Value: yymmddhhmmssZ The date on which the certificate validity period ends Type: UTCTime Value: yymmddhhmmssZ	
Subject		**Value**
CountryName type	Country name attribute of certificate subject Object ID for the country name Type: OID	

	Value: 2 5 4 6	2.5.4.6
value	Value of country name Type: PrintableString	
	Value: JP	JP
OrganizationName	Organization name attribute of certificate subject	
type	Object ID for organization name Type: OID	
	Value: 2 5 4 10	2.5.4.10
value	Value of organization name Type: PrintableString	
	Value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	Common name attribute of certificate subject	
type	Object ID for common name Type: OID	
	Value: 2 5 4 3	2.5.4.3
value	Value of common name Type: PrintableString	
	Value: One of the servers on the right to identify the OCSP server	Cybertrust DeviceiD Public CA G3 OCSP Responder Cybertrust DeviceiD Public CA G3s OCSP Responder Cybertrust DeviceiD Public CA G3k OCSP Responder Cybertrust DeviceiD Public CA G3is OCSP Responder Cybertrust DeviceiD Public CA G3sp OCSP Responder Cybertrust DeviceiD Public CA G3t OCSP Responder Cybertrust DeviceiD Public CA G3h OCSP Responder Cybertrust DeviceiD Public CA G3isr OCSP Responder Cybertrust DeviceiD Education CA G3h OCSP Responder Cybertrust DeviceiD Public CA G3m OCSP Responder Cybertrust DeviceiD Private CA G4pr<xxx> OCSP Responder Cybertrust DeviceiD Premium CA G4pr<xxx> OCSP Responder Cybertrust DeviceiD Premium Root G4pr<xxx> 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	
	Value: 1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	Parameters of cryptographic algorithm Type: NULL	NULL
	Value:	
subjectPublicKey	Public Key Value Type: BIT STRING	
	Value: Public Key Value	*2048Bits

(Certificate Extensions)

basicConstraints (extnId:== 2 5 29 19, critical:== FALSE)		**Value**
BasicConstraints cA	Type: Boolean Value:	FALSE
authorityKeyIdentifier (extnId:== 2 5 29 35, critical:== FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Authority Key Identifier The identifier for public key Type: OCTET STRING	

	Value: Hash value of the Issuer's subjectPublicKey	Following value depending on the Certification Authority CA G3: ED:16:DC:25:12:A8:94:61:7D:8B: 1F:74:C9:D1:E4:D5:F8:08:7C:C0 CA G3s: 01:A1:CF:28:36:47:39:A3:4C:2A: 41:F5:99:84:E4:22:72:28:05:A0 CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC CA G3is: 38:9B:03:06:BA:F7:76:30:ED:16: AC:1A:28:22:33:F2:85:0C:73:54 CA G3sp: B8:79:07:36:4C:FD:24:CD:B3:F6: 0B:F0:07:61:BF:83:12:DC:1A:04 CA G3t: C9:73:E2:3F:C6:0E:72:31:E1:77: 4A:2E:C7:22:7D:C4:FD:24:05:C7 CA G3h: BD:20:46:2C:8C:68:DD:B4:66:28: 31:F2:72:B2:59:2E:32:19:B2:43 CA G3isr: B0:4C:A9:A0:09:F7:0C:C1:94:7C: C0:9D:5D:86:12:99:B8:FC:0E:73 CA G3hedu: 62:38:53:2A:5E:D5:E3:4C:6D:34: 4E:59:E3:47:8E:30:29:E0:BB:D6 CA G3m: A8:B3:38:82:66:EF:14:91:03:8F: 02:30:45:33:56:DD:7A:3F:D8:12 G4pr<xxx>: depends on each CA
subjectKeyIdentifier (extnId:== 2 5 2 14, critical:== FALSE)		**Value**
SubjectKeyIdentifier keyIdentifier	Subject Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of owner's subjectPublicKey	* Hash value of owner's subjectPublicKey
keyUsage (extnId:== 2 5 29 15, critical:== TRUE)		**Value**
KeyUsage	Key Usage Type: BIT STRING Value: 100000000 (digitalSignature)	100000000
extendedKeyUsage (extnId:== 2.5.29.37, critical:== FALSE)		**Value**
extendedKeyUsage	Extended Key Usage Type: OID Value: 1.3.6.1.5.5.7.3.9	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 Type: INTEGER Value: 1	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)	
Algorithm	Object ID for the cryptographic algorithm Type: OID Value: One of the values on the right	CA G2: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2s: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2k: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2is: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2sp: 1.2.840.113549.1.1.5(SHA1withRSA) CA G2t: 1.2.840.113549.1.1.5(SHA1withRSA) CA G3: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3s: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3k: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3is: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3sp: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3t: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3h: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3isr: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3hedu: 1.2.840.113549.1.1.11(SHA256withRSA) CA G3m: 1.2.840.113549.1.1.11(SHA256withRSA) CA G4pr<xxx> 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	Parameters of cryptographic algorithm Type: NULL Value:	NULL
Issuer		**Value**
CountryName	Country name attribute of CRL issuer	
Type	Object ID for the country name Type: OID Value: 2 5 4 6	2.5.4.6
Value	Value of country name Type: PrintableString Value: JP	JP
OrganizationName	Organization name attribute of CRL issuer	
Type	Object ID for organization name Type: OID Value: 2 5 4 10	2.5.4.10
Value	Value of organization name Type: PrintableString Value: Cybertrust Japan Co., Ltd.	Cybertrust Japan Co., Ltd.
CommonName	Common name attribute of CRL issuer	
Type	Object ID for common name Type: OID Value: 2 5 4 3	2.5.4.3
Value	Value of common name Type: PrintableString	

	Value: One of the Certification Authorities on the right to issue the CRL	Cybertrust DeviceiD Public CA G2 Cybertrust DeviceiD Public CA G2s Cybertrust DeviceiD Public CA G2k Cybertrust DeviceiD Public CA G2is Cybertrust DeviceiD Public CA G2sp Cybertrust DeviceiD Public CA G2t Cybertrust DeviceiD Public CA G3 Cybertrust DeviceiD Public CA G3s Cybertrust DeviceiD Public CA G3k Cybertrust DeviceiD Public CA G3is Cybertrust DeviceiD Public CA G3sp Cybertrust DeviceiD Public CA G3t Cybertrust DeviceiD Public CA G3h Cybertrust DeviceiD Public CA G3isr Cybertrust DeviceiD Education CA G3h Cybertrust DeviceiD Public CA G3m Cybertrust DeviceiD Private CA G4pr<xxx> Cybertrust DeviceiD Premium CA G4pr<xxx> Cybertrust DeviceiD Premium Root G4pr<xxx>
thisUpdate		**Value**
thisUpdate	The issue date of this CRL Type: UTCTime or GeneralizedTime Value: yy (2 digit or 4 digit) mmddhhmmssZ	Ex: 090401000000Z
nextUpdate		**Value**
nextUpdate	The date by which the next CRL is issued Type: UTCTime or GeneralizedTime Value: yy (2 digit or 4 digit) mmddhhmmssZ	Ex: 090408000000Z

(CRL Extensions)

authorityKeyIdentifier (extnId:== 2 5 29 35, critical:== FALSE)		**Value**
AuthorityKeyIdentifier keyIdentifier	Authority Key Identifier The identifier for public key Type: OCTET STRING Value: Hash value of Certification Authority's subjectPublicKey	Following value depending on the Certification Authority CA G2: B4:A5:6E:D4:B8:72:AD:F6:E9:AB: EF:63:16:87:41:96:25:3E:0E:DD CA G2s: E3:9B;2A;E6:05;8B:9C:B1:94:6A: BF:6E:20:6B:2D:94:E8:DE:F7:A7 CA G2k: D0:90:B1:59:95:17:3D:78:7C:1B: 24:9F:E9:D3:72:26:4E:81:C4:19 CA G2is: C1:97:3A:C7:22:3A:BA:29:AE:72: 0A:FC:58:5A:86:06:2D:EA:1B:D1 CA G2sp: 15:89:03:9D:B9:D2:C8:4D:04:EC: B4:3E:01:46:73:7D:B0:2B:8C:CA CA G2t: 43:AD:48:61:61:82:22:3B:AE:04: C4:1B:8A:B7:A4:72:0B:D1:28:9B CA G3: ED:16:DC:25:12:A8:94:61:7D:8B: 1F:74:C9:D1:E4:D5:F8:08:7C:C0 CA G3s: 01:A1:CF:28:36:47:39:A3:4C:2A: 41:F5:99:84:E4:22:72:28:05:A0 CA G3k: E8:99:BB:62:F8:41:0D:8F:5B:F8: 80:52:A2:E0:58:06:A4:C2:2C:EC CA G3is: 38:9B:03:06:BA:F7:76:30:ED:16: AC:1A:28:22:33:F2:85:0C:73:54 CA G3sp:

		B8:79:07:36:4C:FD:24:CD:B3:F6: 0B:F0:07:61:BF:83:12:DC:1A:04 CA G3t: C9:73:E2:3F:C6:0E:72:31:E1:77: 4A:2E:C7:22:7D:C4:FD:24:05:C7 CA G3h: BD:20:46:2C:8C:68:DD:B4:66:28: 31:F2:72:B2:59:2E:32:19:B2:43 CA G3isr: B0:4C:A9:A0:09:F7:0C:C1:94:7C: C0:9D:5D:86:12:99:B8:FC:0E:73 CA G3hedu: 62:38:53:2A:5E:D5:E3:4C:6D:34: 4E:59:E3:47:8E:30:29:E0:BB:D6 CA G3m: A8:B3:38:82:66:EF:14:91:03:8F: 02:30:45:33:56:DD:7A:3F:D8:12 CA G4pr<xxx>: depends on each CA
cRLNumber (extnId:== 2 5 29 20, critical:== FALSE)		**Value**
cRLNumber	CRL Number Type: INTEGER Value: Unique Integer	*CRL number

(CRL Entry)

revokedCertificates		**Value**
CertificateSerialNumber	Serial number of revoked certificate Type: INTEGER Value: Unique Integer	*Serial Number
revocationDate	The date on which the revocation occurred Type: UTCTime or GeneralizedTime	

(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 Value: yyyymmddhhmmssZ	*Date and time of revocation processing of corresponding Certificate
cRLReason (extnId:== 2 5 29 21, critical:== FALSE)		**Value**
cRLReason	The reason code for the certificate revocation Type: Enumerated Value: Revocation reason code	(1) keyCompromise (2) cACompromise (3) affiliationChanged (4) superseded (5) cessationOfOperation * “unspecified” is not supported.