Cybertrust

Registration Practices Statement

Version 2.1
June 24, 2019

Cybertrust Japan Co. Ltd.
Roppongi 1-9-10
Ark Hills Sengokuyama Mori Tower, 35th Floor
Tokyo 106-0032
JAPAN

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the Cybertrust Registration Practices Statement (RPS) that outlines the principles and practices related to Cybertrust's participation in DigiCert, Inc.'s certification services. This RPS applies to all entities obtaining digital certificate services through Cybertrust.

As for DigiCert, Inc.'s certification service, DigiCert Certificate Policy (CP) and DigiCert Certificate Practices Statement (CPS) which may be referenced in this document and found at DigiCert Legal Repository (https://www.digicert.com/legal-repository/).

Cybertrust's practices conform to the current version of the following policies, guidelines, and requirements:

- the Certification Authority/Browser Forum ("CAB Forum") Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") located at https://cabforum.org/baseline-requirements-documents/,
- the CAB Forum Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines") located at https://cabforum.org/extended-validation/ ,
- the CAB Forum Network and Certificate System Security Requirements, and
- Mozilla Root Store Policy.

If any inconsistency exists between this RPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this RPS.

This RPS is only one of several documents that control Cybertrust's certification services. Other important documents include both private and public documents, such as the relevant CP, Cybertrust's agreements with its customers, relying party agreements, and the applicable privacy policy. Cybertrust may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this RPS is divided into nine parts that cover the security controls and practices and procedures related to Cybertrust's portion of the certificate issuance and management services. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable".

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the Cybertrust Registration Practices Statement and was first approved for publication on 9 February 2017 by the Cybertrust Policy Authority (CTJ PA).

Date	Changes	Version
17-Febrary-2017	Updated procedure for revocation request	1.01
09-Febrary-2018	Updated by annual review	1.02
20-August-2018	Updated with changes of homepage URL and office address	1.03
15-February-2019	Updated according to RA practices Added section 1.5.2.1 for Revocation Reporting Contact Person and additions/revisions to section 4.9 to meet the revocation requirements for CAB Forum ballot SC6.	2.0
24-June-2019	Edited sections 3.1.6, 3.2.1, 6.1.3, and 7.1.4 to clarify naming and proof-of-possession practices.	2.1

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

Cybertrust is a registration authority for DigiCert, which operates certification authorities (CAs) that issue digital certificates. As a CA, DigiCert performs functions associated with Public Key operations after receiving all appropriate documentation and communication from Cybertrust.

1.3.2. Registration Authorities and Other Delegated Third Parties

Cybertrust is a registration authority participating in the DigiCert PKI. Except for the authentication of domain control or IP address verification performed solely by DigiCert in accordance with Section 3.2.2, DigiCert has delegated the performance of certain functions to Cybertrust as a third party Registration Authority (RA). The Cybertrust RA operates under the CP as applicable to delegated responsibilities. RA personnel involved in the issuance of publicly-trusted SSL/TLS Server Certificates must undergo the skills and training required under Section 5.3.

1.3.3. Subscribers

Subscribers use Certificate services support transactions and communications. Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the Certificate. A *Subscriber*, as used herein, may refer to the Subject of the Certificate and the entity that contracted with Cybertrust for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature verified by DigiCert. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate.

1.3.5. Other Participants

Not applicable.

1.4. CERTIFICATE USAGE

A *digital Certificate* (or C*ertificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this RPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this RPS.

This RPS covers several different types of end entity Certificates with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate	Appropriate Use
OV SSL/TLS Server Certificates	Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
EV SSL/TLS Server Certificates	Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this RPS when the Certificate issued.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This RPS and the documents referenced herein are maintained by the CTJ PA, which can be contacted at:

Cybertrust Policy Authority
Cybertrust Japan Co. Ltd.
Roppongi 1-9-10
Ark Hills Sengokuyama Mori Tower, 35th Floor
Minato-ku, Tokyo 106-0032
JAPAN
+81-3-6234-3800

1.5.2. Contact Person

Attn: Policy Authority
Cybertrust Policy Authority
Cybertrust Japan Co. Ltd.
Roppongi 1-9-10
Ark Hills Sengokuyama Mori Tower, 35th Floor
Minato-ku, Tokyo 106-0032
JAPAN
+81-3-6234-3800

1.5.2.1 Revocation Reporting Contact Person

Attn: Support
DigiCert Support
Cybertrust Japan Co. Ltd.
Roppongi 1-9-10
Ark Hills Sengokuyama Mori Tower, 35th Floor
Minato-ku, Tokyo 106-0032
JAPAN
https://www.cybertrust.ne.jp/support/certificate-problem-reporting.html

Contact for inquiries and complaints is as follows.

・Inquiries about this RPS ・Application process of certificates and technical inquiries	digicert_support@cybertrust.ne.jp
・Revocation requests and inquiries about the revocation request process ・When you have troubles with certificates, find abuses, etc. ・Others (complaints about certificates, etc.)	evc-report@cybertrust.ne.jp

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. Cybertrust will authenticate and log each revocation request according to Section 4.9 of this RPS. Cybertrust will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, Cybertrust will investigate the alleged basis for the

revocation request prior to taking an action in accordance with Section 4.9.1 and 4.9.3.

1.5.3. Person Determining RPS Suitability for the Policy

The CTJ PA determines the suitability and applicability of this RPS based on the results and recommendations received from an independent auditor (see Section 8). The CTJ PA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4. RPS Approval Procedures

The CTJ PA approves the RPS and any amendments. Amendments are made after the CTJ PA has reviewed the amendments' consistency with the CP, by either updating the entire RPS or by publishing an addendum. The CTJ PA determines whether an amendment to this RPS is consistent with the CP, requires notice, or an OID change.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

"Applicant" means an entity applying for a Certificate.

"CAB Forum" is defined in section 1.1.

"Certificate" means an electronic document that uses a digital signature to bind a Public Key and an identity.

"Certificate Approver" is defined in the EV Guidelines.

"Certificate Requester" is defined in the EV Guidelines.

"Contract Signer" is defined in the EV Guidelines.

"Domain Name" is as defined in the Baseline Requirements.

"EV Guidelines" is defined in section 1.1.

"Key Pair" means a Private Key and associated Public Key.

"OCSP Responder" means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

"Private Key" means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

"Public Key" means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

"Relying Party" means an entity that relies upon either the information contained within a Certificate.

"Relying Party Agreement" means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using Cybertrust's Repository.

"Subscriber" means the entity identified as the subject in the Certificate.

"Subscriber Agreement" means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

1.6.2. Acronyms

CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	”CA/Browser” as in “CAB Forum”
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTJ PA	Cybertrust Policy Authority
EV	Extended Validation
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and
Numbers IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PIN	Personal Identification Number (e.g. a secret access
code) PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TTL	Time To Live
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”)

CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (“EV Guidelines”)

Mozilla Root Store Policy v.2.6.1

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

Cybertrust’s legal repository for most services is located at https:// dc.cybertrust.co.jp/repository/.

The repository for CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime. If an SSL/TLS Server Certificate is intended to be trusted in Chrome, it is published by posting it in a Certificate Transparency log.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

Certificate services and the repository are accessible through several means of communication:

1. On the web: https:// dc.cybertrust.co.jp/ (and via URIs included in the certificates themselves)
2. By email to digicert_support@cybertrust.ne.jp
3. By mail addressed to: Cybertrust Japan Co. Ltd., Roppongi 1-9-10 Ark Hills Sengokuyama Mori Tower, 35th Floor Minato-ku, Tokyo 106-0032 JAPAN
4. By telephone Tel: +81-3-6234-3800
5. By fax: +81-11-708-5296

2.3. TIME OR FREQUENCY OF PUBLICATION

New or modified versions of this RPS are typically published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

3.1.2. Need for Names to be Meaningful

Cybertrust uses distinguished names that identify both the entity (i.e. organization) that is the subject of the Certificate and the entity that is the issuer of the Certificate. Cybertrust only allows directory information trees that accurately reflect organization structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, Cybertrust does not permit anonymous or pseudonymous Certificates; however, for IDNs, Cybertrust may authorize inclusion of the Punycode version of the IDN as a subject name. Cybertrust may also authorize other pseudonymous end-entity Certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. *See* RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

SSL/TLS Server Certificates	Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with content that infringes on the intellectual property rights of another entity.

For EV SSL/TLS Certificates, Cybertrust implements a process that prevents EV Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless Cybertrust has verified this information in accordance with the EV Guidelines and section 3.2.

For all other Certificates, unless otherwise specifically stated in this RPS, Cybertrust does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. Cybertrust may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2. INITIAL IDENTITY VALIDATION

Cybertrust may use any legal means of communication or investigation to ascertain the identity of an organizational Applicant. Cybertrust may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

A Certificate Signing Request ("CSR"), a part of the information for the Certificate application submitted by a Subscriber, includes a public key and a digital signature encrypted by corresponding private key.

The Certification Authority verifies the digital signature by using the public key included in the CSR and thereby determines that the subscriber has the private key in possession.

3.2.2. Authentication of Organization and Domain Control

OV SSL/TLS Server Certificates (Domain Verification)	DigiCert validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the procedures listed in section 3.2.2.4 of the Baseline Requirements. DigiCert verifies an included country code using (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar. Verification of country codes included in domains and certificates is conducted by DigiCert in accordance with various guidelines such as Baseline Requirements.
OV SSL/TLS Server Certificates (Organization Verification)	Cybertrust verifies the identity and address of the Applicant using the procedures found in section 3.2.2.1 of the Baseline Requirements. Cybertrust shall use the document/data that is provided by a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition or, a third party database that is periodically updated and considered a Reliable Data Source or, an Attestation Letter. Moreover, Cybertrust shall visit the subscriber and conduct an on-site survey as needed.
EV SSL/TLS Server Certificates	Information concerning organization identity related to the issuance of EV SSL/TLS Server Certificates is validated in accordance with the EV Guidelines.

A scoring system is used to flag certificate requests that potentially present a higher risk of fraud. Those certificate requests that are flagged "high risk" receive additional scrutiny or verification prior to issuance, which may include obtaining additional documentation from or additional communication with the Applicant.

3.2.3. Authentication of Individual Identity

Not applicable.

3.2.3.1. Authentication for Role-based Client Certificates

Not applicable.

3.2.3.2. Authentication for Group Client Certificates

Not applicable.

3.2.3.3. Authentication of Devices with Human Sponsors

Not applicable.

3.2.4. Non-verified Subscriber Information

Cybertrust will not verify the truthfulness and accuracy of the information described in the subscriber's organization unit (OU).

3.2.5. Validation of Authority

The authorization of a certificate request is verified as follows:

Certificate	Verification
OV SSL/TLS Server Certificates	The request is verified using a Reliable Method of Communication, in accordance with section 3.2.5 of the Baseline Requirements.
EV SSL/TLS Server Certificates	The request is verified in accordance with section 11.8.3 of the EV Guidelines.

An organization may limit who is authorized to request Certificates by sending a request to Cybertrust. A request to limit authorized individuals is not effective until approved by Cybertrust. Cybertrust will respond to an organization's verified request for Cybertrust's list of its authorized requesters.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. Rekeying creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, Cybertrust may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
OV SSL/TLS Server Certificates	Username and password	According to the Baseline Requirements
EV SSL/TLS Certificates	Username and password	According to the EV Guidelines

Re-keying a Certificate is not permitted without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial registration process prior to rekeying the Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Cybertrust authenticates all revocation requests. Cybertrust may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Either the Applicant or another requestor authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to Cybertrust.

EV SSL/TLS Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

Certificate issuance is not permitted to entities that receive administrative punishment for prohibition of export from Japan's Ministry of Economy, Trade and Industry.

4.1.2. Enrollment Process and Responsibilities

In no particular order, the enrollment process includes:

1. Submitting a certificate application,
2. Generating a Key Pair,
3. Delivering the Public Key of the Key Pair,
4. Agreeing to the applicable Subscriber Agreement, and
5. Paying any applicable fees.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After receiving a certificate application, Cybertrust verifies the application information and other information in accordance with Section 3.2. Prior to issuing a publicly-trusted SSL/TLS Server Certificate, DigiCert checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. If the Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater. DigiCert processes the "issue" and "issuewild" property tags and may not dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag. CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5.

The Certification Authority CAA identifying domains for CAs within DigiCert's operational control are "digicert.com", "digicert.ne.jp", "cybertrust.ne.jp", "symantec.com", "thawte.com", "geotrust.com", "rapidssl.com", "digitalcertvalidation.com" (with reseller-specific licensed prefixes) and any domain containing those identifying domains as suffixes (e.g. example.digicert.com).

After verification is complete, Cybertrust evaluates the corpus of information and decides whether or not to issue the Certificate. Part of this evaluation includes checking the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

Cybertrust considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable. Cybertrust does not consider a database, source, or form of identification reasonably reliable if Cybertrust is the sole source of the information.

4.2.2. Approval or Rejection of Certificate Applications

Cybertrust rejects any certificate application that Cybertrust cannot verify. Cybertrust may also reject a certificate application if Cybertrust believes that issuing the Certificate could damage or diminish Cybertrust's or DigiCert's reputation or business.

Except for Enterprise EV SSL/TLS Server Certificates, EV SSL/TLS Server Certificate issuance approval requires two separate Cybertrust validation specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV SSL/TLS Server Certificate. The second validation specialist reviews the collected information and documents any discrepancies or details that require further explanation. The second validation specialist may require additional explanations and documents prior to authorizing the Certificate's issuance. Enterprise RAs may perform the final cross-correlation and due diligence described herein using a single person representing the Enterprise RA. If satisfactory explanations and/or additional documents are not received within a reasonable time, Cybertrust will reject the EV SSL/TLS Server Certificate request and notify the Applicant accordingly.

If the certificate application is not rejected and is successfully validated in accordance with this RPS, Cybertrust will approve the certificate application and issue the Certificate. Cybertrust is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

Under normal circumstances, Cybertrust verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL/TLS Server Certificates, Cybertrust will usually complete the validation process within two working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of Cybertrust can delay the issuance process.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

Cybertrust confirms the source of a certificate request before issuance. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Cybertrust may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, Cybertrust sends an email containing a hypertext link that downloads the certificate to the email address designated by the Subscriber during the application process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2. Publication of the Certificate by the CA

End-entity Certificates are published by delivering them to the Subscriber.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Cybertrust receive notification of a Certificate's issuance.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. Cybertrust does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement as applicable.

A Relying Party should rely on SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid

Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked, and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this RPS.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

Cybertrust may request to DigiCert Certificate renewal if:

1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent, and
3. the associated Private Key remains uncompromised.

Cybertrust may notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees.

4.6.2. Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. Cybertrust may elect to reuse previously verified information in its sole discretion but will refresh any information that is older than the periods specified in the Baseline Requirements or EV Guidelines, as applicable.

Cybertrust may refuse to renew a Certificate if it cannot verify any rechecked information. If the Private Key and domain information have not changed, the Subscriber may renew the SSL/TLS Server Certificate using a previously issued Certificate or provided CSR.

4.6.4. Notification of New Certificate Issuance to Subscriber

Cybertrust may deliver the Certificate in any secure fashion, typically by email that contains a hypertext link to a password-protected location where the subscriber may download the Certificate.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6. Publication of the Renewal Certificate by the CA

Renewed Certificates are published by delivering it to the Subscriber.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Cybertrust receives notification of a Certificate's renewal.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same. The new Certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key. Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

4.7.2. Who May Request Certificate Rekey

Cybertrust will only accept re-key requests from the subject of the Certificate or the PKI sponsor. Cybertrust may initiate a certificate re-key at the request of the certificate subject or in Cybertrust's own discretion.

4.7.3. Processing Certificate Rekey Requests

Cybertrust will only accept re-key requests from the subject of the Certificate or the PKI sponsor. If the Private Key and any identity and domain information in a Certificate have not changed, then Cybertrust can request issuance of a replacement Certificate using a previously issued Certificate or previously provided CSR. Cybertrust re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if Cybertrust believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

Cybertrust notifies the Subscriber within a reasonable time after the Certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued Certificates are considered accepted 30 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.7.6. Publication of the Issued Certificate by the CA

Rekeyed Certificates are published by delivering them to Subscribers.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Cybertrust receives notification of a Certificate's rekey.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this RPS. The new Certificate may have the same or a different subject Public Key.

4.8.2. Who May Request Certificate Modification

Cybertrust modifies Certificates at the request of certain certificate subjects or in its own discretion. Cybertrust does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, Cybertrust verifies any information that will change in the modified Certificate. Cybertrust will only issue the modified Certificate after completing the verification process on all modified information. Cybertrust will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4. Notification of Certificate Modification to Subscriber

Cybertrust notifies the Subscriber within a reasonable time after the Certificate issues.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6. Publication of the Modified Certificate by the CA

Modified Certificates are published by delivering them to Subscribers.

4.8.7. Notification of Certificate Modification by the CA to Other Entities

Cybertrust receives notification of a Certificate's modification.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, Cybertrust verifies the identity

and authority of the entity requesting revocation.

Cybertrust will revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that Cybertrust revoke the Certificate;
2. The Subscriber notifies Cybertrust that the original Certificate request had not been authorized and does not retroactively grant authorization;
3. Cybertrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. Cybertrust obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

Cybertrust may request revocation of a certificate within 24 hours and will request revocation of a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CAB forum baseline requirements;
2. Cybertrust obtains evidence that the Certificate was misused;
3. The Subscriber breached a material obligation under DigiCert CP/CPS or this RPS, or the relevant agreement;
4. Cybertrust confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
5. Cybertrust confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. Cybertrust confirms a material change in the information contained in the Certificate;
7. Cybertrust confirms that the Certificate was not issued in accordance with the CAB forum requirements or the DigiCert CP/CPS or this RPS;
8. Cybertrust determines or confirms that any of the information appearing in the Certificate is inaccurate;
9. DigiCert's right to issue Certificates under the CAB forum requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the DigiCert CP/CPS or this RPS; or
11. Cybertrust confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Cybertrust may revoke any Certificate in its sole discretion, including if Cybertrust believes that:

1. Either the Subscriber's or Cybertrust's obligations under the DigiCert CP/CPS or this RPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. Cybertrust received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. DigiCert ceased operations and did not arrange for another Certificate Authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

5. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;

Cybertrust always requests revocation of a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2. Who Can Request Revocation

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

4.9.3. Procedure for Revocation Request

Cybertrust processes a revocation request as follows:

1. Cybertrust logs the identity of entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. Cybertrust may also include its own reasons for revocation in the log.
2. Cybertrust may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, Cybertrust requests Certificate revocation based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, Cybertrust personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate or website,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
5. If Cybertrust determines that revocation is appropriate, DigiCert revokes the Certificate and update the CRL.

If Cybertrust deems appropriate, Cybertrust forwards the revocation reports to law enforcement.

Cybertrust maintains a continuous 24/7 ability to internally respond to any high priority revocation requests.

Cybertrust receives revocation requests at the email address this is written in "1.5.2.1 "Revocation Reporting Contact Person" and/or our portal website.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key.

4.9.5. Time within which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate problem report, Cybertrust investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, Cybertrust works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which Cybertrust will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by Cybertrust will consider the following criteria:

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

2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

Under normal operating circumstances, Cybertrust may request the revocation of Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7. CRL Issuance Frequency

CRLs are published at least every 24 hours. If a Certificate is revoked for reason of key compromise, an interim CRL is published as soon as feasible, but no later than 18 hours after receipt of the notice of key compromise.

4.9.8. Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs are posted within four hours after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

Certificate status information is available via OCSP for SSL/TLS Server Certificates. OCSP may not be available for other kinds of Certificates. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time and no later than six seconds after the request is received, subject to transmission latencies over the Internet.

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements Related to Key Compromise

Certificate will be revoked in accordance with section 4.9.1 of this RPS.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension
Not applicable.

4.9.15. Procedure for Suspension Request
Not applicable.

4.9.16. Limits on Suspension Period
Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics
Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

4.10.2. Service Availability
Certificate status services are available 24x7 without interruption.

4.10.3. Optional Features
OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION
A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy 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
Cybertrust operates a secure data center that is equipped with logical and physical controls that make Cybertrust's operations inaccessible to non-trusted personnel. Cybertrust operates under a security policy designed to detect, deter, and prevent unauthorized access to Cybertrust's operations.

5.1.2. Physical Access

5.1.2.1. Data Centers
Cybertrust protects its operations from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of Cybertrust's facilities are protected using physical access controls making them accessible only to appropriately authorized individuals.

Access to Cybertrust's data centers storing personal information requires two-factor authentication. Activation

data used to perform the RA operations must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module.

5.1.2.2. RA Operations Areas

Controlled access secures the support and vetting rooms where Cybertrust personnel perform identity vetting and other RA functions. Access card use is logged by the building security system.

5.1.2.3. CA Key Generation and Storage

Not applicable.

5.1.3. Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Cybertrust monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available.

5.1.4. Water Exposures

A water leakage detector is installed in the particularly important rooms in the data centers, and waterproofing measures shall be taken.

5.1.5. Fire Prevention and Protection

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

5.1.6. Media Storage

Cybertrust protects its media from accidental damage and unauthorized physical access. Backup files are created on a daily basis. Backup files are maintained at a separate backup site from Cybertrust's data centers.

5.1.7. Waste Disposal

All copies of printed sensitive information are shredded on-site before disposal.

5.1.8. Off-site Backup

Cybertrust maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure.

5.1.9. Certificate Status Hosting, CMS and External RA Systems

Not applicable.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Personnel acting in trusted roles include RA system administration personnel and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.2. Number of Persons Required per Task

Cybertrust requires that at least two people acting in a trusted role take action requiring a trusted role.

5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions; and
3. Those performing audit, review, oversight, or reconciliation functions.

To accomplish this separation of duties, Cybertrust specifically designates individuals to be trusted. Cybertrust's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

The CTJ PA is responsible and accountable for Cybertrust's operations and ensures compliance with this RPS and applicable CP. Cybertrust's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

5.3.2. Background Check Procedures

Where allowed by law, Cybertrust verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role based on the requirements set forth in the guideline on the certificate that Cybertrust verifies and Cybertrust's internal rules and regulations.

5.3.3. Training Requirements

Cybertrust provides skills training to all employees involved in Cybertrust's operations. The training relates to the person's job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by Cybertrust,
3. authentication and verification policies and procedures,
4. Cybertrust security principles and mechanisms,
5. disaster recovery and business continuity procedures,
6. common threats to the validation process, including phishing and other social engineering tactics, and
7. CA/Browser Forum Guidelines and other applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

Cybertrust maintains records of who received training and what level of training was completed. Validation staff must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All validation staff are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of Certificates. Where competence is demonstrated in lieu of training, Cybertrust maintains supporting documentation.

5.3.4. Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs to continue acting in trusted roles. Cybertrust makes all employees acting in trusted roles aware of any changes to Cybertrust's operations. If Cybertrust's operations change, Cybertrust will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

Cybertrust may rotate the jobs of Employees as needed

5.3.6. Sanctions for Unauthorized Actions

Cybertrust employees and agents failing to comply with this RPS, whether through negligence or malicious

intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

Not applicable.

5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the RPS, EV Guidelines, and other technical and operational documentation needed to maintain the integrity of Cybertrust's operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

Cybertrust's systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

Cybertrust enables all essential event auditing capabilities of its RA applications to record the events listed below. If Cybertrust's applications cannot automatically record an event, Cybertrust implements manual procedures to satisfy the requirements. For each event, Cybertrust records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. All event records are available to auditors as proof of Cybertrust's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
MISCELLANEOUS

Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set or modify passwords
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
All certificate compromise notification requests
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Auditable Event
Patches
Security Profiles
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of this RPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

At least once every two months, a Cybertrust administrator reviews the logs generated by Cybertrust's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to Cybertrust's operations management committee and are made available to Cybertrust's auditors upon request. Cybertrust documents any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

Audit logs are retained for at least seven (7) years. Cybertrust retains audit logs on-site until after they are reviewed.

5.4.4. Protection of Audit Log

Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. Cybertrust's off-site storage location is a safe and secure location that is separate from the location where the data was generated. Audit logs are made available to auditors upon request.

5.4.5. Audit Log Backup Procedures

Cybertrust makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the CTJ PA is notified and the CTJ PA will consider suspending the RA's operations until the problem is remedied.

5.4.7. Notification to Event-causing Subject

Cybertrust may collect and investigate the Audit Logs without notification to the party which causes event.

5.4.8. Vulnerability Assessments

Cybertrust performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. Cybertrust also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Cybertrust has in place to control such risks. Cybertrust's Internal Auditors review the security audit data checks for continuity. Cybertrust's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. RECORDS ARCHIVAL

Cybertrust complies with all record retention policies that apply by law.

5.5.1. Types of Records Archived

Cybertrust retains the following information in its archives (as such information pertains to Cybertrust's RA operations):

1. Accreditations of Cybertrust,
2. RPS versions,
3. Contractual obligations and other agreements concerning the operation of the RA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
7. Any documentation related to the receipt or acceptance of a Certificate,
8. Subscriber Agreements,
9. Compliance auditor reports,
10. Changes to Cybertrust's audit parameters,
11. Any attempt to delete or modify audit logs,
12. Appointment of an individual to a trusted role,
13. Remedial action taken as a result of violations of security requirements, and
14. Violations of the RPS.

5.5.2. Retention Period for Archive

Cybertrust retains archived data associated supporting issuance for at least 7.5 years.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the CTJ PA or as required by law. Cybertrust maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If Cybertrust needs to transfer any media to a different archive site or equipment, Cybertrust will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

Cybertrust makes system backups when system change occurs and makes regular system backups at least a once in a quarter-year basis. System backups is hashed to produce checksums that are stored for integrity verification at later date. Cybertrust stores the archive disk in a secure off-site location for the duration of the

set retention period. Cybertrust archives other data to an access-controlled folder, and the server is backed up daily.

5.5.5. Requirements for Time-stamping of Records

Cybertrust automatically time-stamps archived records with system time (non-cryptographic method) as they are created.

5.5.6. Archive Collection System (internal or external)

Archive information is collected internally by Cybertrust.

5.5.7. Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the Cybertrust PKI, Cybertrust may elect to retrieve the information from archival. The integrity of archive information is verified by comparing a hash of the compressed archive file with the file checksum originally stored for that file, as described in Section 5.5.4. Cybertrust may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6. KEY CHANGEOVER

Not applicable.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

Cybertrust maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. Cybertrust reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

Cybertrust makes system backups when system changes occur and makes regular system backups at least a once in a quarter-year basis. If Cybertrust discovers that any of its computing resources, software, or data operations have been compromised, Cybertrust assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If Cybertrust determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, Cybertrust suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

Certificate will be revoked in accordance with section 4.9.1 of this RPS.

5.7.4. Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, Cybertrust implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving Cybertrust's primary facility and that Cybertrust be capable of maintaining other services or resuming them as quickly as possible following a disaster. Cybertrust reviews, tests, and updates the BCMP and supporting procedures at least annually.

5.8. CA OR RA TERMINATION

Before terminating its RA activities, Cybertrust will:

1. Provide notice and information about the termination by sending notice by email to its customers and by posting such information on Cybertrust's web site; and
2. Transfer all responsibilities to a qualified successor entity.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation
Not applicable.

6.1.2. Private Key Delivery to Subscriber
Not applicable.

6.1.3. Public Key Delivery to Certificate Issuer
Subscribers generate Key Pairs and submit the Public Key to DigiCert through Cybertrust in a CSR as part of the certificate request process.

6.1.4. CA Public Key Delivery to Relying Parties
Public Keys for root certificates are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs.

6.1.5. Key Sizes
Subscribers must generate and use at least the following minimum key sizes, signature algorithms, and hash algorithms for all server certs:

2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256) or a hash algorithm that is equally or more resistant to a collision attack.

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)
Certificates include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software. The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Subscriber Certificates assert key usages based on the intended application of the Key Pair. In particular, Certificates to be used for digital signatures (including authentication) set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

Key usage bits and extended key usages are specified in the certificate profile for each type of Certificate as set forth in the applicable Certificate Profiles document.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls
Cybertrust does not manage key pair of Certificate Authority.

6.2.2. Private Key (n out of m) Multi-person Control
Not applicable.

6.2.3. Private Key Escrow
Not applicable.

6.2.4. Private Key Backup
Not applicable.

6.2.5. Private Key Archival
Not applicable.

6.2.6. Private Key Transfer into or from a Cryptographic Module
Not applicable.

6.2.7. Private Key Storage on Cryptographic Module
Not applicable.

6.2.8. Method of Activating Private Keys
Not applicable to the Private Keys for Certificate Authority.

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key.

6.2.9. Method of Deactivating Private Keys
Not applicable to the Private Keys for Certificate Authority.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10. Method of Destroying Private Keys
Not applicable.

6.2.11. Cryptographic Module Rating
Not applicable.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival
Cybertrust archives the copy of Public Keys in accordance with section 5.5 of this RPS.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods
Certificates have maximum validity periods of:

Type	Private Key Use	Certificate Term
Root CA	20 years	25 years
Sub CA	12 years	15 years
CRL and OCSP responder signing	3 years	31 days†
OV SSL/TLS Server	No stipulation	825 days
EV SSL/TLS Server	No stipulation	825 days

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation
All Cybertrust personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. Cybertrust employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis.

6.4.2. Activation Data Protection
All Cybertrust personnel are instructed to memorize and not to write down their password or share it with another individual. Cybertrust locks accounts used to access secure RA processes if a certain number of failed password attempts occur.

6.4.3. Other Aspects of Activation Data
Not applicable.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

Cybertrust secures its RA systems and authenticates and protects communications between its systems and trusted roles. Cybertrust's support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All RA systems are scanned for malicious code and protected against spyware and viruses.

Cybertrust's RA systems, including any remote workstations, are configured to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

6.5.2. Computer Security Rating

Cybertrust preliminarily assesses both of hardware and software to install to RA system. Additionally, Cybertrust continually collects information concerning security vulnerability of the system in use and immediately conduct appropriate measures in the case critical vulnerability has been discovered.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

Cybertrust has mechanisms in place to control and monitor the acquisition and development of its RA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. Cybertrust only installs software on RA systems if the software is part of the RA's operation.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by Cybertrust are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to Cybertrust's operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

Cybertrust has mechanisms in place to control and monitor the security-related configurations of its RA systems. When loading software onto a RA system, Cybertrust verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

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

6.7. NETWORK SECURITY CONTROLS

Cybertrust documents and controls the configuration of its systems, including any upgrades or modifications made. Cybertrust's customer support and vetting workstations are protected by firewall(s) and only use internal IP addresses. Firewalls and boundary control devices are configured to allow access only by the

addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

Cybertrust's security policy is to block all ports and protocols and open only ports necessary to enable RA functions. All RA equipment is configured with a minimum number of services and all unused network ports and services are disabled. Cybertrust's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8. TIME-STAMPING

Time-Stamping is practiced in accordance with Section 5.5.5 in this RPS.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Certificates are ITU X.509, version 3 standard digital certificates. Cybertrust adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

7.1.2. Certificate Extensions

Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId; the same certificate does not include both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds.

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

7.1.3. Algorithm Object Identifiers

Certificates are signed using one of the following algorithms:

sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]

Cybertrust does not issue publicly trusted SSL/TLS Server Certificates to a Reserved IP address or Internal Name.

7.1.4. Name Forms

Each Certificate includes a unique serial number that is never reused. Optional subfields in the subject of an SSL Certificate must either contain information verified by Cybertrust or be left empty. SSL/TLS Server Certificates cannot contain metadata such as '.', '-', and ' ' characters and/or any other indication that the value/field is absent, incomplete, or not applicable. Cybertrust logically restricts OU fields from containing Subscriber information that has not been verified in accordance with Section 3.

The contents of the fields in EV SSL/TLS Server Certificates must meet the requirements in Section 8.1 of the EV Guidelines

7.1.5. Name Constraints

Name constraints may be included in the nameConstraints field when appropriate.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by Cybertrust are assigned based on the Certificate type and are established in the applicable Certificate profile.

7.1.7. Usage of Policy Constraints Extension
Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics
Certificates may include a brief statement about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension
Not applicable.

7.2. CRL PROFILE

7.2.1. Version number(s)
Certificates authorized by Cybertrust use Version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR
Issuer Distinguished Name	DigiCert
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL Entry Extensions
CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3. OCSP PROFILE

7.3.1. Version Number(s)
OCSP responders conform to version 1 of RFC 6960.

7.3.2. OCSP Extensions
Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
The practices in this RPS are designed to meet or exceed the requirements of generally accepted industry standards.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT
Cybertrust receives an annual period in time audit by an independent external auditor to assess Cybertrust's compliance with this RPS.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR
WebTrust auditors must meet the requirements of Section 8.2 of the Baseline Requirements.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY
Cybertrust's auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against Cybertrust.

8.4. TOPICS COVERED BY ASSESSMENT

The audit covers Cybertrust's business practices disclosure and Cybertrust's compliance with this RPS and referenced requirements.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, the RPS, or any other contractual obligations related to Cybertrust's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify Cybertrust, and (3) Cybertrust will develop a plan to cure the noncompliance. Cybertrust will submit the plan to the CTJ PA for approval and to any third party that Cybertrust is legally obligated to satisfy. The CTJ PA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates.

8.6. COMMUNICATION OF RESULTS

The results of each audit are reported to the CTJ PA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7. SELF-AUDITS

On at least a quarterly basis, Cybertrust performs regular internal audits against a randomly selected sample of at least three percent of the OV SSL/TLS Server Certificates and at least six percent of the EV SSL/TLS Certificates issued since the last internal audit. Self-audits on server Certificates are performed in accordance with Guidelines adopted by the CA / Browser Forum.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

Cybertrust charges fees for certificate issuance and renewal. Cybertrust may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

Cybertrust may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation or Status Information Access Fees

Cybertrust does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL.

9.1.4. Fees for Other Services

Not applicable.

9.1.5. Refund Policy

Refund policy is as set forth in the Certificate Subscriber Agreement.

9.2. FINANCIAL RESPONSIBILITY

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

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

1. Business continuity, incident response, contingency, and disaster recovery plans;

2. Other security practices used to protect the confidentiality, integrity, or availability of information;
3. Information held by Cybertrust as private information in accordance with Section 9.4;
4. Audit logs and archive records; and
5. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this RPS).

9.3.2. Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

Cybertrust's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information.

9.4.2. Information Treated as Private

Cybertrust treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. Cybertrust protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Not Deemed Private

Private information does not include Certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

Cybertrust employees and contractors are expected to handle personal information in strict confidence. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. Cybertrust will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Cybertrust may disclose private information, without notice, if Cybertrust believes the disclosure is required by law or regulation.

9.4.7. Other Information Disclosure Circumstances

Not applicable.

9.5. INTELLECTUAL PROPERTY RIGHTS

Cybertrust and/or its business partners own the intellectual property rights in Cybertrust's services, including the Certificates, trademarks used in providing the services, and this RPS.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

Not applicable

9.6.2. RA Representations and Warranties

Cybertrust represents that:

1. Cybertrust's certificate issuance and management services conform to the Cybertrust RPS and DigiCert CP,
2. Information provided by Cybertrust does not contain any false or misleading information,
3. All Certificates requested by Cybertrust meet the requirements of the applicable CP.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify Cybertrust and the issuance CA if a change occurs that could affect the status of the Certificate.

Cybertrust requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of Cybertrust and the Certificate Beneficiaries. Prior to the issuance of a Certificate, Cybertrust will obtain, for the express benefit of Cybertrust and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with Cybertrust, or
2. The Applicant's acknowledgement of the Terms of Use.

Subscribers represent to Cybertrust, DigiCert, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with Cybertrust,
3. Confirm the accuracy of the certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify Cybertrust if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this RPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL/TLS Server Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and
7. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.
8. Refrain from using a certificate in which a name, trade name, trademark, address, location and any other value for referring to a specific natural person, a judicial person other than those of the subscriber, meta data such as '.', '-', and ' ' (i.e. space) characters, or any other indication that the value is absent, incomplete, or not applicable is included in the organization unit (OU) included in the certificate.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a Certificate, it:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to the applicable limitations on liability related to the use of Certificates,
3. Has read, understands, and agrees to the applicable Relying Party Agreement and CP,
4. Verified both the Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a Certificate if the Certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:
    a) applicable law and the legal requirements for identification of a party, protection of the

confidentiality or privacy of information, and enforceability of the transaction;
b) the intended use of the Certificate as listed in the certificate or the applicable CP,
c) the data listed in the Certificate,
d) the economic value of the transaction or communication,
e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
f) the Relying Party's previous course of dealing with the Subscriber,
g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5. Representations and Warranties of Other Participants

Not applicable.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, CYBERTRUST AND DIGICERT DISCLAIM ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. CYBERTRUST AND DIGICERT DO NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. Cybertrust does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an entity uses Cybertrust's services.

9.8. LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM CYBERTRUST'S NEGLIGENCE OR (II) FRAUD COMMITTED BY CYBERTRUST. EXCEPT AS STATED ABOVE, ANY ENTITY USING A CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF CYBERTRUST OR DIGICERT RELATED TO SUCH USE, PROVIDED THAT CYBERTRUST AND DIGICERT HAVE MATERIALLY COMPLIED WITH THIS RPS IN PROVIDING THE CERTIFICATES OR SERVICES. CYBERTRUST'S AND DIGICERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS RPS OR THE APPLICABLE CP IS LIMITED AS SET FORTH IN THE CYBERTRUST'S AGREEMENT.

All liability is limited to actual and legally provable damages. Neither DigiCert nor Cybertrust is liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if a party is aware of the possibility of such damages;
2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or the applicable CP;
4. Liability related to the security, usability, or integrity of products not supplied by Cybertrust, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether a DigiCert or Cybertrust failed to follow any provision of the applicable CP, or (v) whether any provision of the applicable CP was proven ineffective.

The disclaimers and limitations on liabilities in this RPS are fundamental terms to the use of the Certificates and services.

9.9. INDEMNITIES

9.9.1. Indemnification by Cybertrust
Not applicable.

9.9.2. Indemnification by Subscribers
To the extent permitted by law, each Subscriber shall indemnify Cybertrust, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, the applicable CP, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3. Indemnification by Relying Parties
To the extent permitted by law, each Relying Party shall indemnify Cybertrust, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, the applicable CP, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. TERM AND TERMINATION

9.10.1. Term
This RPS and any amendments to the RPS are effective when published to Cybertrust's online repository and remain in effect until replaced with a newer version.

9.10.2. Termination
This RPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival
Cybertrust will communicate the conditions and effect of this RPS's termination via the Cybertrust Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the Certificate is revoked or expired, even if this RPS terminates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS
Cybertrust accepts notices related to this RPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from Cybertrust. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. Cybertrust may allow other forms of notice in its Subscriber Agreements.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment
This RPS is reviewed annually. Controls are in place to reasonably ensure that this RPS is not amended and published without the prior authorization of the CTJ PA.

9.12.2. Notification Mechanism and Period
Cybertrust does not guarantee or set a notice-and-comment period and may make changes to this RPS without notice and without changing the version number.

9.12.3. Circumstances under which OID Must Be Changed
Not applicable.

9.13. DISPUTE RESOLUTION PROVISIONS

Parties are required to notify Cybertrust and attempt to resolve disputes directly with Cybertrust before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

The laws of Japan govern the interpretation, construction, and enforcement of this RPS for all proceedings related to Cybertrust's products and services, including tort claims, without regard to any conflicts of law principles. The courts located in Japan have non-exclusive venue and jurisdiction over any proceedings related to the RPS or Cybertrust's services.

9.15. COMPLIANCE WITH APPLICABLE LAW

This RPS is subject to all applicable laws and regulations.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

Cybertrust requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this RPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this RPS may not assign their rights or obligations without the prior written consent of Cybertrust. Unless specified otherwise in a contact with a party, Cybertrust does not provide notice of assignment.

9.16.3. Severability

If any provision of this RPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the RPS will remain valid and enforceable. Each provision of this RPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Cybertrust may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Cybertrust's failure to enforce a provision of this RPS does not waive

Cybertrust's right to enforce the same provision later or right to enforce any other provision of this RPS. To be effective, waivers must be in writing and signed by Cybertrust.

9.16.5. Force Majeure

Cybertrust is not liable for any delay or failure to perform an obligation under this RPS to the extent that the delay or failure is caused by an occurrence beyond Cybertrust's reasonable control. The operation of the Internet is beyond Cybertrust's reasonable control.

9.17. OTHER PROVISIONS

Not applicable.