Cybertrust

Registration Practices Statement

Version 1.01
February 17, 2017

Cybertrust Japan Co. Ltd.
Akasaka 1-12-32
Ark Mori, 30th Floor
Minato-ku, Tokyo 107-6030
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.

Cybertrust's practices conform to the current version of the guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") when participating in the issuance of publicly trusted Certificates, including the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") and the Guidelines for Extended Validation Certificates ("EV Guidelines"), both of which are published at https://www.cabforum.org. With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between this RPS and the Baseline Requirements or the EV Guidelines, then the EV Guidelines take precedence for EV Certificates and the Baseline Requirements take precedence for publicly trusted SSL Certificates.

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 and time-stamping services. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation."

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

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 CTTJ.

1.3.2. Registration Authorities and Other Delegated Third Parties

Cybertrust is a registration authority participating in the DigiCert PKI. DigiCert has delegated the performance of certain functions to Cybertrust as a Registration Authority (RA), including the authority to request Certificates and/or perform identification and authentication for end-user Certificates. The Cybertrust RA operates under the CP as applicable to Cybertrust's role in certificate issuance, management, revocation or other related tasks.

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, refers to both 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 Cybertrust. 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

No stipulation.

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/tokens 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 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 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.
Code Signing Certificates, including EV Code Signing	Establishes the identity of the Subscriber named in the Certificate and that the signed code has not been modified since signing.
Rudimentary Level 1 Client Certificates - Personal	Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These Certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.

Level 1 Client Certificates - Enterprise	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 2 Client Certificates	Issued to identity-vetted individuals. Certificates specify if the name is a pseudonym. Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 3 Client Certificates	Used in environments where 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.
Level 4 Client Certificates	Used in environments where risks and consequences of data compromise are high, including transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high.
Authentication Only	Used where the identity of the certificate holder is irrelevant and where the risk of unauthorized access to a secure site is low.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued. Code signing Certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

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.
Akasaka 1-12-32
Ark Mori, 30th Floor
Minato-ku, Tokyo 107-6030
JAPAN
+81 3-6234-3800

1.5.2. Contact Person

Attn: Policy Authority
Cybertrust Policy Authority
Cybertrust Japan Co. Ltd.
Akasaka 1-12-32
Ark Mori, 30th Floor
Minato-ku, Tokyo 107-6030
JAPAN
+81 3-6234-3800

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	evc-report@cybertrust.ne.jp

・When you have troubles with certificates , find abuses, etc. ・Others (complaints about certificates, etc.)	

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

"Affiliated Organization" means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a Certificate.

"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.

"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 Cybertrust 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 or a time-stamp token.

"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 either 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

AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAB	"CA/Browser" as in "CAB Forum"
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
CTJ PA	Cybertrust Policy Authority
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDN	Internationalized Domain Name
ISSO	Information System Security Officer
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
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
PKCS	Public Key Cryptography Standard
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
URL	Uniform Resource Locator
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")

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

Cybertrust's legal repository for most services is located at https://www.digicert.ne.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.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

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

1. On the web: https://www.digicert.ne.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., Akasaka 1-12-32, Ark Mori, 30th Floor, Minato-ku, Tokyo 107-6030 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 the 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 except that a Level 1 Certificate may contain a null subject DN if it includes at least one alternative name form that is marked critical. 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. Some SSL/TLS Certificates, including Certificates for intranet use and Multi-SAN Certificates, may contain entries in the subject alternative name extension that are not intended to be relied upon by the general public (e.g., they contain non-standard top level domains like .local or they are addressed to an IP number space that has been allocated as private by RFC1918). The issuance of publicly-trusted SSL Certificates to these local IP addresses or with non-FQDN (DNS-addressable) server names has been deprecated. Cybertrust may authorize issuance of EV SSL/TLS Certificates to .onion domains in accordance with Appendix F of the EV Guidelines.

3.1.2. Need for Names to be Meaningful

Cybertrust uses distinguished names that identify both the entity (i.e. person, organization, device, or object) 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 provided that 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 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).
Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.
Code Signing Certificates (including CDS Certificates)	Requiring a unique organization name and address or a unique organization name combined/associated with a unique serial integer.

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 OSU Server Certificates and in accordance with section 4.1.7 of the Hotspot 2.0 CP, Cybertrust conducts a trademark search of logos and Friendly Names in relevant mark registration databases, such as the U.S. Patent and Trademark Office or WIPO, to confirm an applicant's right to use a particular trademark. Based on the results of such search(es), Cybertrust issues an OSU Server Certificate with one or more logotype extensions containing the hash algorithm and hash value of logos associated with the service provider, in accordance with RFC 3709 and section 3.4 of the Hotspot 2.0 CP. If an applicant does not have a friendly name or logo available, Cybertrust may include a logo and friendly name specified by the Wi-Fi Alliance.

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 or individual Applicant. Cybertrust may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

Cybertrust establishes that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

3.2.2. Authentication of Organization Identity

SSL Server Certificates (Domain Verification)	Cybertrust or its partners validate the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the procedures permitted by the Baseline Requirements, including: 1. Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information; 2. Communicating with one of the following email addresses:

	webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed in the technical, registrant, or administrative contact field of the domain's Registrar record; 3. Requiring a practical demonstration of domain control using the .well-known directory; 4. A domain authorization letter, provided the letter contains the signature of an authorized representative of the domain holder, a date that is on or after the certificate request, a list of the approved fully-qualified domain name(s), and a statement granting the Applicant the right to use the domain names in the Certificate. Cybertrust also contacts the domain name holder using a reliable third-party data source to confirm the authenticity of the domain authorization letter; and/or 5. A similar procedure that offers an equivalent level of assurance in the Applicant's ownership, control, or right to use the Domain Name as permitted under the Baseline Requirements. Cybertrust 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.
SSL Server Certificates (Organization Verification)	Cybertrust validates the Applicant's right to use or control the Domain Name(s) that will be listed in the Certificate using the Domain Verification procedures above. Cybertrust also verifies the identity and address of the Applicant using: 1. a reliable third party/government databases or through communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition; 2. a site visit; 3. an attestation letter that is signed by an accountant, lawyer, government official, or other reliable third party; or 4. for address only, a utility bill, bank statement, credit card statement, tax document, or other reliable form of identification.
EV SSL and EV Code Signing Certificates	Information concerning organization identity related to the issuance of EV Certificates is validated in accordance with the EV Guidelines.
Level 1 Client Certificate	Cybertrust verifies organizational control over the email domain using authentication procedures similar to those used by Cybertrust when establishing domain ownership by an organization before issuance of a SSL Server Certificate.
Level 2, 3, and 4 Client Certificates	If the Certificate contains organization information, Cybertrust obtains documentation from the organization sufficient to confirm that the individual has an affiliation with the organization named in

	the Certificate.

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

If a Certificate will contain the identity of an individual, then Cybertrust validates the identity of the individual using the following procedures:

Certificate	Validation
SSL Server Certificates and Object Signing Certificates (where issued to an individual)	1. Cybertrust obtains a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). Cybertrust inspects the copy for any indication of alteration or falsification. 2. Cybertrust may additionally cross-check the Applicant's name and address for consistency with available third party data sources. 3. If further assurance is required, then the Applicant must provide an additional form of identification, such as recent utility bills, financial account statements, credit card, an additional ID credential, or equivalent document type. 4. Cybertrust confirms that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If Cybertrust cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
OSU Server Certificates	Cybertrust verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
EV Certificates issued to a business entity	As specified in the EV Guidelines
Authentication-Only Certificates	The entity controlling the secure location must represent that the certificate holder is authorized to access the location.
Level 1 Client Certificates – Personal (email Certificates)	Cybertrust verifies the Applicant's control of the email address or website listed in the Certificate.
Level 1 Client Certificates - Enterprise	Any one of the following: 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in

	consumer credit databases or government records, such as: a. the ability to place or receive calls from a given number; or b. the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method used to verify the identity of an Applicant for a Level 2, 3, or 4 Client Certificate.
Level 2 Client Certificates	The RA confirms that the following are consistent with the application and sufficient to identify a unique individual: (a) the name on the government-issued photo-ID referenced below; (b) date of birth; and (c) current address or personal telephone number. 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID. 2. The Applicant must possess a valid, current, government-issued, photo ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks with an agent/institution or through credit bureaus or similar databases. Cybertrust may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records available to Cybertrust.

	3. Where Cybertrust has a current and ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods used to verify the identity of an applicant for a Cybertrust Level 3 or 4 Client Certificate.
Level 3 Client Certificates	In-person proofing before Cybertrust, a Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. The information must be collected and stored in a secure manner. Required identification consists of one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The person performing identity proofing examines the credentials and determines whether they are authentic and unexpired and checks the provided information (name, date of birth, and current address) to ensure legitimacy. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. Cybertrust or the RA reviews and keeps a record of the Declaration of Identity. Cybertrust also employs the in-person antecedent process, defined in FBCA Supplementary Antecedent, In-Person Definition, to meet this in-person identity proofing requirement. Under this definition, historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, the Applicant (e.g. an employee) has been identified previously by an employer using USCIS Form I-9 and is bound to the asserted identity remotely through the use of known attributes or shared secrets. In another use case, Cybertrust uses a third party Identity Verification Provider that constructs a real-time, five-question process, based on multiple historic antecedent databases, and the applicant is given two minutes to answer at least four of the five questions correctly. See FBCA Supplementary Antecedent, In-Person Definition. The identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.
Level 4 Client Certificates (Biometric ID Certificates)	In-person proofing before Cybertrust, a Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. A certified entity must forward the collected

	information directly to Cybertrust in a secure manner. The Applicant must supply one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D.. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The entity collecting the credentials must also obtain at least one form of biometric data (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application. The person performing identity verification for Cybertrust examines the credentials for authenticity and validity. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. Cybertrust reviews and keeps a record of the Declaration of Identity. Use of an in-person antecedent is not allowed. The identity of the Applicant must be established by in-person proofing no earlier than 30 days prior to initial certificate issuance. Level 4 Client Certificates are issued in a manner that confirms the Applicant's address.

A Declaration of Identity consists of:

1. the identity of the person performing the verification;
2. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law, the signature on the declaration may be either a handwritten or digital signature using a Certificate that is of equal or higher level of assurance as the credential being issued;
3. unique identifying number(s) from the Applicant's identification document(s), or a facsimile of the ID(s);
4. the date of the verification; and
5. a declaration of identity by the Applicant that is signed (in handwriting or using a digital signature that is of equivalent or higher assurance than the credential being issued) in the presence of the person performing the verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

If in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate of the same type applied for by the Applicant. The person accompanying the Applicant (i.e. the "Sponsor") will present information sufficient for registration at the level of the Certificate being requested, for himself or herself, and for the Applicant.

For in-person identity proofing at Levels 3 and 4, Cybertrust may rely on an entity certified by a state, federal, or national entity as authorized to confirm identities may perform the authentication on behalf of the RA. The certified entity should forward the information collected from the applicant directly to the RA in a secure manner.

3.2.3.1. Authentication for Role-based Client Certificates

Certificates may identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). These role-based Certificates are used when non-repudiation is desired. Cybertrust only

issues role-based Certificates to Subscribers who first obtain an individual Subscriber Certificate that is at the same or higher assurance level as the requested role-based Certificate. Certificates may be issued with the same role to multiple Subscribers. However, each Certificate must have a unique Key Pair. Individuals may not share their issued role-based Certificates and are required to protect the role-based Certificate in the same manner as individual Certificates.

Cybertrust verifies the identity of the individual requesting a role-based Certificate (the sponsor) in accordance with Section 3.2.3 before issuing a role-based Certificate. The sponsor must hold a DigiCert-issued client individual Certificate at the same or higher assurance level as the role-based Certificate. If the Certificate is a pseudonymous Certificate cross-certified with the FBCA that identifies subjects by their organizational roles, then Cybertrust validates that the individual either holds that role or has the authority to sign on behalf of the role.

Regarding the issuance of role-based Certificates, this RPS requires compliance with all provisions of the applicable CP regarding key generation, private key protection, and Subscriber obligations.

3.2.3.2. Authentication for Group Client Certificates

Group Certificates (a Certificate that corresponds to a Private Key that is shared by multiple Subscribers) are permitted if several entities are acting in one capacity and if non-repudiation is not required. The sponsor for these Certificates must be at least an Information Systems Security Officer (ISSO) or of the equivalent rank or greater within the organization.

The sponsor is responsible for ensuring control of the Private Key. The sponsor must maintain and continuously update a list of Subscribers with access to the Private Key and account for the time period during which each Subscriber had control of the key. Group Certificates may list the identity of an individual in the subjectName DN provided that the subjectName DN field also includes a text string, such as "Direct Group Cert," so that the Certificate specifies the subject is a group and not a single individual. Client Certificates issued in this way to an organization are always considered group client Certificates.

3.2.3.3. Authentication of Devices with Human Sponsors

Level 1, 2, 3 or 4 Client are issued if the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment Public Keys,
3. Equipment authorizations and attributes (if any are to be included in the Certificate), and
4. Contact information.

If the Certificate's sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive Certificates. Each sponsor is required to provide proof that the device is still under the sponsor's control or responsibility on request. Sponsors are contractually obligated to notify Cybertrust if the equipment is no longer in use, no longer under their control or responsibility, or no longer requires a Certificate. All registration is verified commensurate with the requested certificate type.

3.2.4. Non-verified Subscriber Information

Level 1 - Personal Client Certificates are verified by email, and the common name is not verified as the legal name of the Subscriber. Cybertrust does not authorize issuance of SSL Certificates to domain names or IP addresses that a Subscriber does not legitimately own or control. Cybertrust may rely on the Subscriber's indication of the host or server name that forms the fully qualified domain name. Any other non-verified information included in a Certificate is designated as such in the Certificate. 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
SSL Server Certificates	The request is verified using a Reliable Method of Communication, in accordance with the Baseline Requirements.
OSU Server Certificates	Cybertrust verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
EV Certificates	The request is verified in accordance with the EV Guidelines.
Object Signing Certificates and Adobe Signing Certificates	If the Certificate names an organization, the requester's contact information is verified with an authoritative source within the applicant's organization using a Reliable Method of Communication. The contact information is then used to confirm the authenticity of the certificate request.
Level 1 Client Certificates Personal (email Certificates)	The request is verified through the email address listed in the Certificate.
Level 1 Client Certificates – Enterprise (email Certificates)	The request is verified with a person who has technical or administrative control over the domain and the email address to be listed in the Certificate.
Client Certificates Levels 2, 3 and 4	The organization named in the Certificate confirms to Cybertrust that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.

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
Non-EV SSL Server Certificates	Username and password	At least every 39 months
EV SSL Certificates	Username and password	According to the EV Guidelines
Subscriber EV Code Signing Certificates	Username and password	At least every 39 months
Signing Authority EV Code Signing Certificates	Username and password	At least every 123 months
Subscriber EV Code Signing Certificates	Username and password	At least every 123 months
Object Signing Certificates (including Adobe Signing Certificates)	Username and password	At least every six years
Level 1 Client Certificates	Username and password	At least every nine years
Level 2 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years

Level 3 and 4 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Authentication-Only Certificates	Username and password or with associated Private Key	None

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 an individual 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 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. During the initial validation process, Cybertrust or its partners checks the DNS for the existence of a CAA record. If a CAA record exists that does not list Cybertrust as an authorized CA, Cybertrust verifies that the applicant has authorized issuance, despite the CAA record. 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 Certificates, EV 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 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 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 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 delivers Certificates via email 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 a digital signature or 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 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. Cybertrust may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

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 Section 3.3.1. Cybertrust may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then Cybertrust does not require any additional identity vetting. Some device platforms, e.g. Apache, allow renewed use of the Private Key. If the Private Key and domain information have not changed, the Subscriber may renew the SSL 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 or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and 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 may request revocation of any Certificate in its sole discretion if Cybertrust believes that:

1. The Subscriber requested revocation of its Certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised or misused;
4. The Subscriber breached a material obligation under the CP, the RPS, or the relevant Subscriber Agreement;
5. Either the Subscriber's or Cybertrust's obligations under the CP or 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;
6. The Subscriber, sponsor, or other entity that was issued the Certificate has lost its rights to a name, trademark, device, IP address, domain name, or other attribute that was associated with the Certificate;
7. A wildcard Certificate was used to authenticate a fraudulently misleading subordinate domain name;
8. The Certificate was not issued in accordance with the CP, RPS, or applicable industry standards;
9. Cybertrust received a lawful and binding order from a government or regulatory body to revoke the Certificate;
10. DigiCert ceased operations and did not arrange for another certificate authority to provide revocation support for the Certificates;

11. Cybertrust's right to manage Certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
12. Any information appearing in the Certificate was or became inaccurate or misleading;
13. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;
14. 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;
15. For Adobe Signing Certificates, Adobe has requested revocation; or
16. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

A Certificate is always revoked 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. 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.
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.

Cybertrust maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, Cybertrust forwards complaints to law enforcement. Cybertrust receives revocation requests at the email address this is written in "1.5.2 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

Certificates are revoked as quickly as practical after validating the revocation request, 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 and all CRLs for CAs chaining to the Federal Bridge 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 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

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

No stipulation.

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, except for revoked EV Code Signing Certificates, which remain on the CRL for at least 365 days following 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

Cybertrust may escrow Subscriber key management keys to provide key recovery services. Cybertrust encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key.

Cybertrust allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. Cybertrust uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. Cybertrust accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the private-key token;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with Cybertrust for Private Key escrow;
3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with Cybertrust for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using Cybertrust's key escrow services are required to:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

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

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 secure areas of the buildings requires the use of an "access" or "pass" card. Cybertrust securely stores all removable media and paper containing sensitive plain-text information related to its operations in secure containers in accordance with its Data Classification Policy.

5.1.2.1. Data Center

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. Support and Vetting Room

Controlled access secure 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.

5.1.3. 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

No stipulation.

5.1.5. Fire Prevention and Protection

No stipulation.

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 locations separate from Cybertrust's primary data operations facility.

5.1.7. Waste Disposal

All unnecessary 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

No stipulation.

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. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the Cybertrust 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 principals 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. 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

No stipulation.

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

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

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

Auditable Event
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
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

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 sends a copy of the audit log off-site on 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

No stipulation.

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 or token,
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

On at least an annual basis, Cybertrust creates an archive disk of the data listed in section 5.5.1 by grouping the data types together by source into separate, compressed archive files. Each archive file is hashed to produce checksums that are stored separately for integrity verification at a later date. Cybertrust stores the archive disk in a secure off-site location for the duration of the set retention period. RAs create and store archived records in accordance with the applicable documentation retention policy.

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

No stipulation.

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 regular system backups on at least a weekly 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

No stipulation.

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

All keys must be generated using a FIPS-approved method or equivalent international standard. Subscribers must generate their keys in a manner that is appropriate for the certificate type.

6.1.2. Private Key Delivery to Subscriber

If Cybertrust generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module / SSCD. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery,
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and
4. The key generator must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
    b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers generate Key Pairs and submit the Public Key to Cybertrust in a CSR as part of the certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the Certificate.

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 or
256-bit ECDSA 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

No stipulation.

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

Cryptographic modules for the CA and OCSP responder Key Pairs used in providing certificate services are validated to the FIPS 140 Level 3 and International Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) 14169 EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in the European Union (EU).

Cryptographic module requirements for subscribers and registration authorities are shown in the table below.

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Adobe Signing	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 3 (Hardware)
Level 1 Client	N/A	FIPS 140 Level 1 (Hardware or Software)

Level 2 Client	FIPS 140 Level 1 (Hardware or Software)	FIPS 140 Level 1 (Hardware or Software)
Level 3 Client	FIPS 140 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Level 4 Client	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)

The Private Key of an EV Code Signing Certificate requirement is met by Cybertrust or DigiCert (i) shipping conforming cryptomodules with preinstalled Key Pairs, (ii) communicating via PKCS#11 crypto APIs of cryptomodules that the Subscriber meets or exceeds requirements, or (iii) obtaining an IT audit from the Subscriber that indicates compliance with FIPS 140-2 level 2 or the equivalent. All other keys may be stored in software.

6.2.2. Private Key (n out of m) Multi-person Control
Cybertrust's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

6.2.3. Private Key Escrow
Cybertrust does not escrow signature keys.

6.2.4. Private Key Backup
No stipulation.

6.2.5. Private Key Archival
Cybertrust does not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module
All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form.

6.2.7. Private Key Storage on Cryptographic Module
Private Keys for the root certificates are generated and stored inside a cryptographic module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+.

6.2.8. Method of Activating Private Keys
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. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys.

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

6.2.10. Method of Destroying Private Keys
No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

No stipulation.

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	No stipulation	39 months
EV SSL	No stipulation	27 months
Code Signing Certificate and Document Signing	No stipulation‡	123 months
EV Code Signing Certificate issued to Subscriber	No stipulation	39 months
EV Code Signing Certificate issued to Signing Authority	123 months	123 months
Adobe Signing Certificate	39 months	5 years
End Entity / Client	No Stipulation	60 months

Code signers may use their Private Keys for three years; the lifetime of the associated Public Keys shall not exceed eight years. Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

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

No stipulation.

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

No stipulation.

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

No stipulation.

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.

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

No stipulation.

7.1.3. Algorithm Object Identifiers

Certificates are signed using one of the following algorithms:

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

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 Certificates cannot contain metadata such as '.', '-' and ' ' characters or any other indication that the field is not applicable.

7.1.5. Name Constraints

No stipulation.

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

No stipulation.

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-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
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 2560.

7.3.2. OCSP Extensions

No stipulation.

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 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 14.1.14 of the EV Guidelines. Specifically:

(1) *Qualifications and experience*: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential. Auditors must be subject to disciplinary action by its licensing body.

(2) *Expertise*: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.

(3) *Rules and standards*: The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), CPA Canada, the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

(4) *Reputation*: The firm must have a reputation for conducting its auditing business competently and correctly.

(5) *Insurance*: EV auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

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 policy document.

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 Non-EV SSL Certificates and at least six percent of the EV SSL and EV Code Signing Certificates issued since the last internal audit. Self-audits on SSL and code signing 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

No stipulation.

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

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets
No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities
No stipulation.

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

No stipulation.

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

No stipulation

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. 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 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 or a judicial person other than those of the subscriber 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

No stipulation.

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 FOLLOWS:

1. NO LIABILITY IF THE DAMAGE OR LOSS RELATES TO A CERTIFICATE OTHER THAN A SSL CERTIFICATE OR CODE SIGNING CERTIFICATE,
2. A MAXIMUM LIABILITY OF $1,000 PER TRANSACTION FOR SSL CERTIFICATES,
3. AN AGGREGATE MAXIMUM LIABILITY OF $10,000 FOR ALL CLAIMS RELATED TO A SINGLE CERTIFICATE OR SERVICE,
4. AND AN AGGREGATE MAXIMUM LIABILITY OF $1 MILLION FOR ALL CLAIMS, REGARDLESS OF THE NUMBER OR SOURCE OF THE CLAIMS.

Cybertrust AND DIGICERT APPORTION PAYMENTS RELATED TO AN AGGREGATE MAXIMUM LIMITATION ON LIABILITY UNDER THIS SECTION TO THE FIRST CLAIMS THAT ACHIEVE FINAL RESOLUTION.

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

No stipulation.

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

No stipulation.

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 and 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

No stipulation.