verizonbusiness
Security Solutions powered by Cybertrust

CA Certificate Policy

for Cybertrust Certification Services

Date: April 22, 2016

Version: v.2.7

Table of Contents

Document History

Version	Date	Name	Action
V2.0	30.06.05	Andreas Mitrakas	Second version
V 2.1	26.01.07	Johan Sys	Distributed to Policy Board
V 2.2	04.06.07	Johan Sys	Administrative Update
V 2.3	11.09.07	Jean-Paul Declerck	Align with CPS v5.3
V 2.4	22.07.13	Steven Medin	Align with CPS v5.5 (Unpublished)
V2.5	27.04.14	Stephane Mans-Zunz	Align with CPS v5.6
V2.6	13.01.15	Steven Medin	Administrative update
V2.7	22.04.16	Stephane Mans-Zunz	Align with CPS v5.8

Acknowledgments

This Cybertrust CA CP endorses in whole or in part the following industry standards:

- CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements
- CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFCs 2459, 3280, 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- The ISO 1-7799 standard on security and infrastructure
- CA/Browser Forum Certificate Guidelines version 1.3.4 and prior versions during their effective periods as well as future versions as they take effect.
- CA/Browser Forum EV Certificate Guidelines version 1.5.9 and prior versions during their effective periods as well as future versions as they take effect.
- CA / Browser Forum Network and Certificate System Security Requirements, v. 1.0

This CP has been submitted for assessment of compliance with the requirements of the above-mentioned standards. This CP is assessed according to the requirements of the following schemes:

- AICPA/CICA, WebTrust Program for Certification Authorities, WebTrust for Extended Validation Certification Authorities.

1. Introduction

This Certificate Policy (CP) of the Cybertrust Certification Authority (hereinafter, Cybertrust CA) applies to the services of the Cybertrust CA that are associated with the issuance of and management of digital certificates issued under the Top Roots managed by Cybertrust. Top Root certificates can be used to manage certificate hierarchies of certification authorities as well as of end entity certificates. This CP can be found on the Cybertrust CA repository at: https://secure.omniroot.com/repository. This CP may be updated from time to time.

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". This CP is a certificate policy in broad sense and meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format (RFC 3647 obsoletes RFC 2527). An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and certificate management. While certain section titles are included in this policy according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the certificate management services of the Cybertrust CA. These sections have been omitted. Where necessary additional information is presented as subsections added to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability of the Cybertrust CA with other third party CAs and provides relying parties with advance notice on the practices and procedures of the Cybertrust CA. Additional assertions on standards used in this CP can be found under section “Acknowledgements”.

This CP addresses the technical, procedural personnel policies and practices of the CA in certain services and during the complete life cycle of off line certificate solutions that are issued by the Cybertrust CA.

Request for information on the compliance of the Cybertrust CA with accreditation schemes as well as any other inquiry associated with this CP can be addressed to:

Cybertrust Belgium nv/sa
Verizon Enterprise Solutions
Attn. Head of Information Security
Culliganlaan 2E
1831 Diegem
Belgium
Email: EVServiceDesk@verizonbusiness.com
URL: www.verizon.com/ssl

The Cybertrust CA operates within the scope of activities of Cybertrust Belgium nv/sa, a wholly owned affiliate of Verizon Business Global Services LLC. This CP addresses the requirements of the CA that issues top level certificates. Top-level certificates are also known as root certificates or anchor certificates. The Cybertrust CA also issues other certificate types at varying levels of its hierarchy. More information can be obtained from https://secure.omniroot.com/repository.

This CP applies in all cases of offline solutions that are associated with the CA chaining services called OmniRoot that Cybertrust makes available. The Verizon wholly owned subsidiary Omniroot LLC is the owner and custodian of the roots operated in association with this CP. This CP also

applies in cases related with the validation of the certificate path for certificates that are issued at lower levels in the Cybertrust hierarchy like for example end entity certificates.

For subscribers this CP becomes effective and binding by accepting a subscriber agreement. For subscribers seeking CA chaining services this CP becomes effective by executing a CA chaining agreement with Cybertrust for any of the roots that Cybertrust owns or manages under license. For relying parties this CP becomes binding by merely addressing a certificate related request on a Cybertrust certificate to a Cybertrust directory or accessing a device secured by such a certificate. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CP.

1.1 Overview

This CP applies to the specific domain of the Cybertrust CA that addresses the management of top level or root certificates issued under Cybertrust's own procedures. The purpose of this CP is to present the Cybertrust practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of top root certificates according to Cybertrust's own procedures as they are audited in the framework of formal accreditations that it currently pursues. This CP applies to the above-stated domain to the exclusion of any other. This CP aims at facilitating the Cybertrust CA in delivering certification services through discrete CAs issuing end entity certificates. This certificate type is known as Cybertrust OmniRoot.

This CP sets out the objectives to identify the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of root certificates of Cybertrust. This CP describes the policy requirements to issue, manage and use Cybertrust root certificates. As a root CA, Cybertrust manages a hierarchy of intermediate issuing CA and end entity certificates according to published practices at https://secure.omniroot.com/repository.

A CP states "what is to be adhered to" and, therefore, sets out an operational rule framework for the broad range of Cybertrust products and services. Such framework is generally defined by the entity wishing to ensure a level of trust by managing the life cycle of digital certificates. The Cybertrust CP addresses the requirements of the entire application domain of Cybertrust certificates focusing on root certificates and their entire hierarchy and not just the end entity tier.

A Cybertrust Certificate Practice Statement complements this CP and states, "how the Certification Authority adheres to the Certificate Policy". The Certificate Practice Statement provides the end user with a summary of the processes, procedures and overall prevailing conditions that the Certification Authority will use in creating and maintaining digital certificates it manages. Cybertrust maintains a single Certification Practice Statement for all types of end entity certificates.

In addition to the CP and Certificate Practice Statement, Cybertrust maintains a number of adjacent policies. Such policies may relate to:

- Business continuity
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

External policies binding certificate applicants, subscribers, and relying parties are made available online at https://secure.omniroot.com/repository, or at such other place Cybertrust may indicate.
A subscriber or relying party of a Cybertrust CA certificate must refer to the Cybertrust CP in order to establish trust of a certificate issued by the Cybertrust Root CA as well as for notices with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the Cybertrust certificate hierarchy, including the root CA and operational intermediates, which can be established on the basis of the assertions of this CP.

All applicable Cybertrust policies have been subjected to continuous audit and scrutiny of authorised third parties. Additional information can be made available upon request.

The exact names of the Cybertrust CA certificates that make use of this CP are

- Baltimore Cybertrust Root expiring in 2025
- Cybertrust Global Root expiring in 2021 and 2030
- Verizon Global Root expiring in 2034

They are called collectively the Cybertrust CA Roots. OmniRoot is the Cybertrust service which allows third-party CA to chain to one of the Cybertrust CA Roots.

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign and/or encrypt data electronically. By means of a digital certificate, Cybertrust provides confirmation of the relationship between a named entity (subscriber) and its public key.

One type of end entity with regard to Cybertrust position in the relationship is a subscribing third party Certification Authority that seeks to enter the Cybertrust hierarchy. The purpose of entering the Cybertrust hierarchy enhances trust in the hierarchy as well as greater functionality within third party applications such as browsers etc. Cybertrust seeks to maintain a position of leadership with regard to inclusion of its roots in third party applications. This endeavour does not undermine, however, the ability of Cybertrust to revise its approach and seek alternative strategies in the future.

The other type of end entity subscribes to obtain certificates that identify people and devices such that a relying party may accept Cybertrust's external verification of the identity asserted in such certificates.

The process to obtain a digital certificate includes the identification, naming, authentication and registration of the client as well as aspects of certificate management such as the issuance, revocation and expiration of the digital certificate. By means of this procedure to issue digital certificates, Cybertrust provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such entity uses. An entity on this instance might include an end use or another certification authority, as it might be required under the circumstances. Cybertrust makes available general purpose digital certificates that can be used for non-repudiation and authentication. The use of these certificates can be further limited to a specific business or contractual context or transaction level according a warranty policy or other limitations imposed by the applications in which the certificates are used.

This CP is maintained by the Cybertrust CA, which is the issuing authority of certificates in the Cybertrust Public Key Infrastructure. In a certificate management environment based on Public Key Infrastructure (PKI), an Issuing Authority is the entity that manages a trust hierarchy from which all end user certificates inherit Trust.

This CP governs the issuance of Cybertrust OmniRoot subordinated CA certificates during the application period of the Cybertrust CA Roots. An application period is for example, the time during which a certain CA may issue Cybertrust CA certificates. The application period is indicated in the certificate issued to the Cybertrust OmniRoot by a hierarchically superior CA within the Cybertrust hierarchy.

This CP governs the issuance of Cybertrust end entity certificates during the application period of the Cybertrust OmniRoot subordinated CA certificates.

This CP is made available online in this repository: https://secure.omniroot.com/repository.

The Cybertrust CA accepts comments regarding this CP addressed to the address mentioned above in the Introduction of this document.

1.1.1 Cybertrust OmniRoot

This CP addresses the requirements for Cybertrust OmniRoot to be used by appropriately authorized certification authorities that seek to enter the certificate hierarchy of Cybertrust. Entering the Cybertrust hierarchy is carried out through a CA chaining program that Cybertrust makes available to interested parties. OmniRoot certificates:

- Are issued by Cybertrust to a third party CA that meets the contractual and policy requirements of Cybertrust OmniRoot services with regard to operational practices and technical implementation.
- Are issued to enterprise and commercial CAs.
- Enable SSL server, S/MIME, and code signing certificate issuance.
- Are either audited to WebTrust or ETSI 102 142 standards, in the process of being audited to these standards, or constrained by inclusion of name constraints and extended key usage extensions.
- Are NOT permitted for use in man in the middle packet inspection use cases under any circumstances.

1.1.2 Certificate usages

Certain limitations apply to the use of Cybertrust OmniRoot and OmniRoot certificates which typically allow for authentication of the third party CA within an application environment in order to facilitate relying parties in establishing the identity of the CA.

1.1.3 OmniRoot end entities

This CP addresses the requirements for end entity certificates issued under Cybertrust OmniRoot CAs and their use within the PKI community.

1.2 Document Name and Identification

By including an object identifier in a certificate Cybertrust assures of its conformance with the identified certificate policy requirements published in ETSI TS 102 042.

The identifiers for the certificate policies specified in this CP are defined with the scope of the 1.3.6.1.4.1.6334.1.0 arc.

1.3 PKI participants

1.3.1 Cybertrust Certification Authority

A Certification Authority is an organisation that issues digital certificates that are used in the public domain or within a business or transactions context. Cybertrust is a Certification Authority. Sometimes, a certification authority is also described by the term issuing authority.

Cybertrust is also responsible to draft the policy prevailing in issuing a certain type or class of digital certificate. Cybertrust is also a Policy Authority while this Certificate Policy is a policy for the issuance of Cybertrust OmniRoot certificates.

To provide notice or knowledge to relying parties functions associated with the revoked and/or suspended certificates requires appropriate publication in a certificate revocation list. Cybertrust operates such a list.

A subject of Cybertrust CA chaining services is a third party CA that successfully contracts with Cybertrust on the delivery of root services. Root certificates are issued for the purpose of authenticating the trust anchor of a hierarchy as well as the certification path prior to relying on a digital certificate issued by a hierarchically lower CA. Any other uses of root certificates are restricted.

Root certificates can be used for any public purposes. As “public”, this CP considers any use that takes place among CAs that is not restricted to uses governed by voluntary agreements under private law among participants. Closed user groups are also permitted to leverage the Cybertrust hierarchy.

The Cybertrust CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates. The Cybertrust CA is a Policy Authority with regard to issuing Cybertrust CA certificates. The Cybertrust CA has ultimate control over the lifecycle and management of the Cybertrust CA Root and any subsequent root belonging to its hierarchy.

The Cybertrust CA ensures the availability of all services pertaining to the management of certificates under the Cybertrust CA Root, including without limitation the issuing, revocation, and status verification of a certificate including Cybertrust OmniRoot, as they may become available or required in specific applications. The Cybertrust CA also manages a registration system for all certificate types issued under the Cybertrust CA Root or intermediate OmniRoot CAs.

Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of functions associated with the revoked and/or suspended certificates. Publication is manifested by including a revoked or suspended certificate in a certificate revocation list that is published in an online directory. Issued certificates also appear in directories of issued certificates. The Cybertrust CA operates such directories.

The domain of responsibility of the Cybertrust CA’s comprises of the overall management of the certificate lifecycle including the following actions:

- Issuance

- Revocation
- Re-key
- Status validation
- Directory service

Some of the tasks attributed to the certificate lifecycle are delegated to select Cybertrust RAs that operate on the basis of a service agreement with Cybertrust as explained below under 1.3.2.

1.3.1.1 Cybertrust agents

Cybertrust relies on Verizon Enterprise Solutions organizational agents to operate a secure facility and deliver CA services including the issuance, suspension, revocation, and status validation of Cybertrust CA certificates. The Cybertrust agents operate a service to Cybertrust on the basis of a service agreement. Verizon Enterprise Solutions is wholly owned by the same parent organization as Cybertrust.

1.3.1.2 Roles of Cybertrust

Cybertrust operates as a Trust Service Provider to deliver Trust Services to a user community, directly or through an agent. An agent in this case includes third party entities, called Registration Authorities (RAs) that operate under agreement with and within the conditions laid out by Cybertrust.

The Cybertrust public certification services aim at supporting secure electronic commerce and on-line business services and to address the business and personal requirements of the users of electronic signatures.

1.3.1.3 Cybertrust roots and hierarchy

Cybertrust makes available to subscribers dedicated root hierarchies to ensure the integrity of the end user certificate and the uniqueness of the resources that it makes available. The Cybertrust CA Roots belong to the broader domain of the Cybertrust trust network that includes roots that have been set up to fulfill specific purposes such as the issuance of end user certificates following processes defined by Cybertrust as well as other participating CAs that take advantage of Cybertrust's root, which is embedded in applications. This Cybertrust Certificate Policy addresses the Root and intermediate tiers of the Cybertrust hierarchy and provides guidance with regard to the general conditions of the Cybertrust services.

The Cybertrust CA Root has been used to certify each of the private keys of the subsequent third party intermediate CAs. By validating the certificate of such a CA, trust vested in Cybertrust can also be extended to the certified third party CA. The Cybertrust CA Root has issued intermediate CAs operated by Cybertrust for the purposes of issuing end entity certificates.

1.3.2 Cybertrust Registration Authorities

The Cybertrust CA reaches its subscribers through designated Registration Authorities. An RA requests the issuance, suspension and revocation of a certificate under this CP.

An RA submits the necessary data for the generation and revocation of the certificates to the CA.

A Cybertrust RA interacts with the subscriber to deliver public certificate management services to the end-user. A Cybertrust RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to Cybertrust CA certification services.
- Attends all stages of the identification of subscribers as assigned by the Cybertrust CA according to the type of certificates they issue.
- Uses official, notarised or otherwise authorised documents to evaluate a subscriber application.
- Following approval of an application, notifies the Cybertrust CA to issue a certificate.
- Initiates the process to suspend, unsuspend or revoke a certificate and request a certificate revocation from the Cybertrust CA.

The Cybertrust RA acts locally on approval and authorisation by the Cybertrust CA. The Cybertrust RA acts in accordance with the approved practices and procedures of the Cybertrust CA including this CP and documented Cybertrust RA procedures. Verizon Enterprise Solutions operates an RA under the Cybertrust CA for the purposes of end entity certificate issuance.

1.3.3 Subscribers

Subscribers of Cybertrust OmniRoot are third party CAs that seek to be issued with certificates within a hierarchy managed by Cybertrust. Subscribers also include natural and legal persons acting as operators of devices who seek to obtain a trusted identity verification of a device and its ownership, as well as natural persons who seek a trusted verification of their identity.
Subscribers are parties that:

- Set the framework of providing certification services with the Cybertrust CA to the benefit of the subject mentioned in a certificate.
- Have ultimate authority over the private key corresponding to the public key that is listed in a subject certificate.
- Accept and implement the contractual, audit and policy requirements of Cybertrust Omniroot services with regard to operational practises and technical implementation.

Legal persons must be duly represented by an authorised agent (e.g. an authorised Director). Legal persons cannot be mentioned as subjects for an OmniRoot intermediate CA certificate.

1.3.4 Subjects

Subjects of Cybertrust OmniRoot are third party CAs and end entities that seek to be issued with certificates within a hierarchy managed by Cybertrust.

Subjects use electronic signature services under authorisation of and within the domain that is designated by the subscriber (if applicable). Subjects are parties that:

- Apply for a certificate.
- Are identified in a certificate.
- Hold the private key corresponding to the public key that is listed in a subscriber certificate.

A subject enrolls with the Cybertrust RA or a service provider that requires it to use a certificate within the designated service. A subject nominates a named Certificate Applicant also called a Subscriber, to apply for a certificate. A certificate applicant can be any natural person acting on behalf of the subject.

Subjects of Cybertrust CA root certificates are the same as the applying organisation, which is either the third party CA that requests Cybertrust for CA chaining services or the end entity certificate applicant.

1.3.5 Certificate Applicants

A Certificate Applicant is a party wishing to become a subscriber of a certificate. A certificate Applicant is a party designated by the subject to act on the subject's behalf in:

- Applying for a certificate.
- Agreeing with and accepting the relevant CA's subscriber agreement.

The applicant may be:

- The same as the subject itself, where this is a named individual.
- An individual employed by the subject.
- An individual employed by a contractor, or sub-contractor acting upon explicit authorisation.

1.3.6 Relying Parties

Relying parties are natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate. For example, the Cybertrust operators that receive signed requests from Cybertrust CA subjects are relying parties of the Cybertrust certificates.

To verify the validity of a digital certificate, relying parties must always refer to CA revocation information, currently a Certificate Revocation List (CRL). Validation takes place prior to relying on information featured in a certificate. Alternatively, relying parties may refer to an automated response by using the OCSP protocol where available. Relying parties meet specific obligations as described in this CP.

1.4 Certificate use

Certain limitations apply to the use of Cybertrust CA and end entity certificates.

1.4.1 Appropriate certificate usage

Root certificates issued under the Cybertrust CA can be used to issue digital certificates for public domain transactions that require:

- Authentication
- Assurance about the identity of a remote device
- Encryption of data at rest or in transit
- Digital signatures

Additional uses are specifically designated once they become available to end entities. Unauthorised use of Cybertrust CA certificates may result in an annulment of warranties offered by the Cybertrust CA to subscribers and relying parties.

1.4.2 Prohibited certificate usage

End entity certificate use is restricted by using certificate extensions to specify key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not permitted.

1.4.3 Certificate extensions

Cybertrust root certificate extensions are defined by the X.509 v.3 standard and other standards as well as any other formats including those used by common user agents such as browsers and mobile devices.

Cybertrust uses certain constraints and extensions for its public PKI services as per the definition of the International Standards Organisation (ISO). Such constraints and extensions may limit the role and position of a CA or subscriber certificate so that such subscribers can be identified under varying roles.

The key usage extension limits the technical purposes for which a public key listed in a certificate may be used. Cybertrust's own certificates may contain a key usage extension that limits the functionality of a key to only signing certificates, certificate revocation lists, or other data.

A certificate policy extension limits the usage of a certificate to the requirements of a business or a legal context. Cybertrust pro-actively supports and participates in the proliferation of industry, government or other certificate policies for its public certificates as it sees appropriate.

1.4.4 Critical Extensions

Cybertrust uses certain critical extensions in the certificates it issues such as:

- A basic constraint in the key usage to show whether a certificate is meant for a CA or not.
- To show the intended usage of the key.
- To show the number of levels in the hierarchy under a CA certificate.

1.5 Policy Administration

The Cybertrust CA is a root authority (also known as trust anchor) that manages certificates services within its own domain. The Cybertrust CA might also interact with or seek recognition by third party certification authorities.

The Policy Managing Authority of the Cybertrust CA manages this CP. The Cybertrust CA registers, observes the maintenance of, and interprets this CP. The Cybertrust CA makes available the operational conditions prevailing in the life cycle management of certificates issued under the Cybertrust CA root. The operational conditions for each root are publicised in this CP.

1.5.1 Scope

In an effort to invoke credibility and trust in the publicised Cybertrust CP and to better correspond to accreditation and legal requirements, Cybertrust may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all

certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CP and/or CPS.

1.5.2 Cybertrust Policy Management Authority

New versions and publicized updates of Verizon Cybertrust policies are approved by the Verizon-Cybertrust Policy Management Authority. The Verizon-Cybertrust Policy Management Authority in its present organisational structure comprises members as indicated below:

- At least one member of the management of Cybertrust.
- At least two authorised agents directly involved in the drafting and development of Cybertrust practices and policies.

The Management member chairs the Verizon-Cybertrust Policy Management Authority ex officio.

All members of the Verizon-Cybertrust Policy Management Authority have one vote. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chair of the Verizon-Cybertrust Policy Management Authority counts double.

1.5.3 Acceptance of Updated Versions of the CP

Upon approval of a CP update by the Cybertrust Policy Management Authority that CP is published in the Cybertrust online Repository at https://secure.omniroot.com/repository.

The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CP is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the Cybertrust CP.

Subscribers that are affected by changes may file comments with the policy administration organization within 15 days from notice. Only subscribers and the supervisory authority may submit objections to policy changes. Relying parties that are not subscribers do not have the right to submit objections and any such submissions will be regarded as never received.

Cybertrust publishes on its web site at least the two latest versions of its CP.

1.5.3.1 Changes with notification

Updated versions of this CP are notified to auditors as necessary.

1.5.4 Version management and denoting changes

Changes are denoted through new version numbers for the CP. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.6 Definitions and acronyms

A list of definitions can be found at the end of this CP.

2. Publication and Repository Responsibilities

Cybertrust publishes information about the digital certificates that it issues in an online publicly accessible repository. Cybertrust reserves its right to publish certificate status information in third party repositories.

Cybertrust retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CP. Cybertrust reserves its right to make available and publish information on its policies by any appropriate means within the Cybertrust repository.

All parties who are associated with the issuance, use or management of Cybertrust certificates are hereby notified that Cybertrust may publish submitted information on publicly accessible directories in association with the provision of electronic certificate status information.

Cybertrust refrains from making publicly available certain elements of documents including security controls, procedures, and internal security policies. However, these elements are disclosed in audits associated with formal accreditation schemes to which Cybertrust adheres.

2.1 Access control on repositories

While Cybertrust strives to keep access to its public repository and access to its policy (e.g. CP, CPS etc.) free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc.

3. Identification and Authentication

Cybertrust maintains documented practices and procedures to authenticate the identity and/or other attributes of an end-user certificate applicant to a Cybertrust CA or Cybertrust RA prior to issuing a certificate. The details of these practices and procedures are set forth in the Certificate Practice Statement corresponding to this Certificate Policy, as the specific practice varies depending on the intended use of the certificate.

Cybertrust uses approved procedures and criteria to accept applications from entities seeking to become Cybertrust CAs, RAs, or other entities operating in or interoperating with Cybertrust's infrastructure including entities seeking CA chaining services.

Cybertrust authenticates the requests of parties wishing the revocation of certificates under this policy.

Cybertrust maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names and logos.

3.1 Naming

To identify a subscriber Cybertrust follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names.

When applying for a OmniRoot certificate, the applicant's name must be meaningful unless explicitly permitted in the relevant product description and the Cybertrust CP. Cybertrust issues certificates to applicants submitting a documented application containing a verifiable name.

3.2 Initial Identity Validation

The identification of the applicant for Cybertrust services including CA chaining services is carried out according to a documented procedure that is implemented by the Cybertrust RAs.

The subscriber identified in the subject field must prove possession of the private key corresponding to the public key being registered with Cybertrust. Such a relationship can be proved by, for example, a digital signature in the certificate signing request message.

Cybertrust accepts other CAs wishing to enter its own network and operate under its own hierarchy. Following an initial assessment and the signing of a specific agreement with Cybertrust the applicant CA has to provide Cybertrust with certain identification documents including an authorisation letter and articles of incorporation. Cybertrust retains its right to consult third party databases that identify organisations in this regard.

CA chaining services do not require the physical appearance of the customer as long as an agreement between the applicant organisation and Cybertrust has been executed.

The identification of the applicant for end entity certificates is carried out according to a documented procedure that is implemented by the Cybertrust RAs.

The subscriber identified in the subject field must prove possession of the private key corresponding to the public key being registered with Cybertrust. Such a relationship can be proved by, for example, a digital signature in the certificate signing request message.

Cybertrust RAs will prove exclusive ownership and control of the identities asserted in an end entity certificate using governmental databases and commercial aggregates of these databases deemed to be updated at a pace that ensures accuracy.

Device domain name assignments are managed by ICANN, which Cybertrust RAs validate using a WHOIS service. Trademarks, service marks, trade names and registered versions of these are managed by various international patent and trademark offices and aggregated by commercial database providers to which Cybertrust RAs may subscribe.

3.3 Subscriber registration process

Cybertrust manages and operates the service to be compliant to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and the Guidelines for Extended Validation Certificates as available at https://www.cabforum.org.

Cybertrust makes reasonable efforts to ensure that:

- Subscribers are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.

In particular:

- Cybertrust provides notice to the applicant through the dedicated policy framework published on its repository at https://secure.omniroot.com/repository.
- Before entering any contractual relationship with a CA subscriber, Cybertrust makes available a CA chaining agreement, which the applicant must approve prior to placing a request with Cybertrust.
- Cybertrust's policy framework is limited under data protection and consumer protection laws and applicable warranty limitations, as explained in this Cybertrust CP.
- Cybertrust maintains documented contractual relationships with all third party registration authorities or outsourced agents it uses to deliver certificates.

3.3.1 Documents used for subscriber registration

Cybertrust or an authorized Cybertrust RA verifies by appropriate means and on the basis of a documented procedure, the identity and, if applicable, all specific attributes thereof of applicants of a certificate. In addition to the above, to identify organizations Cybertrust typically requests certified copies of by-laws, and possibly additional identification elements such as proof of VAT registration etc.

3.3.2 Data needed for subscriber registration

For CA chaining services, evidence required might include:

- Full name (including surname and given names) of the subscriber.

- Date and place of birth, a nationally recognized identity number, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.

For end entity certificate services, evidence required might include:

- Full name (including surname and given names) of the subscriber.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.

3.3.3 Pseudonyms

Pseudonyms are not permitted for Cybertrust OmniRoot certificates.

3.3.4 Records for subscriber registration

Cybertrust records all information used to verify the subscriber identity, including any reference number on the documentation used for verification, and any limitations on the validity thereof.

Cybertrust maintains records of the executed CA chaining contract and any material or documents that support the application which also might include but is not limited to:

- CA chaining agreement as approved of and executed by the applicant.
- Consent to the keeping of a record by Cybertrust of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CP in the case of the CA terminating its services.
- A statement to the effect that information held in the certificate is correct and accurate.
- Full name of the subscriber.
- Proof of organization context.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.

Cybertrust maintains records of the executed subscriber agreement and any material or documents that support the application for an end entity certificate which also might include but is not limited to:

- Consent to the keeping of a record by Cybertrust of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CP in the case of the CA terminating its services.

- A statement to the effect that information held in the certificate is correct and accurate.
- Full name of the subscriber.
- Proof of organizational context.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.
- Data gathered by Cybertrust RAs independently from authoritative device domain ownership databases and commercial data aggregators who accurately report the records of authoritative government agencies.

The records identified above shall be kept for a period of no less than five (5) years following the expiration of a certificate as mandated by business documentation legislation. A Cybertrust RA maintains such records.

3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests of OmniRoot certificates, Cybertrust requires a written and undersigned statement of the subscriber requesting the revocation.

For the identification and authentication procedures of revocation requests of end entity certificates, Cybertrust requires either a written and undersigned statement of the subscriber requesting the revocation, or execution of a request using a shared secret initiated by the subscriber at the time of enrolment.

4. Certificate Life-Cycle Operational Requirements

All entities within the Cybertrust domain including third party CAs, RAs and subscribers or other participants, have a continuous duty to inform the Cybertrust CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or is revoked.

The Cybertrust CA issues, revokes or suspends certificates following an authenticated and duly signed request issued by a Cybertrust RA.

Cybertrust manages and operates the service to be compliant to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the Guidelines for Extended Validation Certificates, and the CA / Browser Forum Network and Certificate System Security Requirements, v. 1.0 as available at https://www.cabforum.org.

4.1 Certificate Application

The application process for an OmniRoot intermediate CA certificate requires the execution of a CA chaining agreement with Cybertrust. Subsequently the applicant sends to Cybertrust through secure dispatch the required registration data as well as the public key to be included in a subordinate certificate. The Cybertrust RA validates the identity of the applicant on the basis of credentials presented prior to requesting the issuance of a subordinate certificate by the Cybertrust CA.

The application process for an end entity certificate requires the execution of a subscriber agreement with Cybertrust. Subsequently the applicant sends to Cybertrust through secure dispatch the required registration data as well as the public key to be included in an end entity certificate. The Cybertrust RA validates the identity of the applicant and subscriber on the basis of information and credentials provided as well as correlating this information to publicly available authoritative data sources.

4.2 Certificate Application Processing

For all certificate types, a Cybertrust RA acts upon a certificate application to validate an applicant's identity. Subsequently, an RA either approves or rejects a certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

The RA uses documented and audited procedures and adopts its own practices.

4.3 Certificate Issuance

Further to validation and approval of a certificate application, the Cybertrust RA sends a certificate issuance request to the Cybertrust CA.

Requests from the RA are granted approval provided that they are validly made and they contain valid subscriber data, formatted according the Cybertrust CA specifications.

Issued certificates are delivered to the subject.

4.4 Certificate generation

With reference to the issuance of certificates, Cybertrust represents towards all parties that certificates are issued securely according to the conditions set below:

- The procedure to issue a certificate, including a subordinate certificate, is securely linked to the associated registration, including the provision of any subscriber generated public key.
- Certificate generation for CA certificates is done in an offline ceremony, conforming to Webtrust for CA standards for key generation and maintenance and physical and logical security controls.
- Cybertrust ensures the uniqueness of the distinguished name assigned to the subscriber within its own domain.
- The confidentiality and integrity of registration data is ensured at all times through appropriate means.
- The authentication of RA registrars is ensured through appropriate credentials.
- Certificate requests and generation are also supported by robust and tested procedures.
- If external registration service providers are used, registration data is exchanged with authenticated registration service providers.
- Cybertrust accepts independent audits of its services and practices.

4.5 Certificate Acceptance

An issued Cybertrust CA certificate is deemed accepted by the subscriber when the RA confirms the acceptance of a certificate the CA issues.

Objection to accepting an issued certificate must explicitly be notified to the Cybertrust CA within 5 working days from delivery. Thereafter the certificate is deemed accepted.

The Cybertrust CA might publish issued certificates.

4.6 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

4.6.1 Subscriber

The obligations of the subscriber include the following ones:

4.6.1.1 Subscriber duties

The duties of subscribers include the following:

1. Accepting all applicable terms and conditions in the CP of Cybertrust published in the Cybertrust Repository.

2. Notifying the Cybertrust CA or a Cybertrust RA of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a Cybertrust certificate when it becomes invalid.
4. Using a Cybertrust certificate, as it may be reasonable under the circumstances.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
6. Using secure devices and products that provide appropriate protection to their keys and which were approved prior by Cybertrust.
7. Accepting responsibility for any acts and omissions of partners and agents as subscribers used to generate, retain, escrow, or destroy any private keys.
8. Refraining from submitting to Cybertrust or any Cybertrust directory any material that contains statements that violate any law or the rights of any party.
9. Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a Cybertrust certificate.
10. Refraining from tampering with a certificate.
11. Only using certificates for legal and authorised purposes in accordance with the CP and either the CA chaining agreement or applicable subscriber agreement.

The Subscriber has all above stated duties towards the CA at all times. When the subscriber applies on behalf of a different named Subject certain duties can be mitigated to the Subject, which in return shall have to inform the Subscriber of any eventualities affecting the life cycle of a certificate. In such case of mitigation, duties 2, 3, 4, 5, 6, 8, 9 10, 11 above apply to the Subject and not to the Subscriber.

4.6.1.2 Certificate Life-Cycle Operational Requirements

Subscribers have a continuous duty to inform directly a Cybertrust RA of any and all changes in the information featured in a certificate during the validity period of such certificate or of any other fact that materially affects the validity of a certificate. This duty can be exercised either directly by the subscriber of through an agent.

4.6.1.3Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the Cybertrust CA Repositories and web site to assess and rely on information featured therein.

4.6.2 Relying party

The duties of a relying party are as follows:

4.6.2.1Relying party duties

A party relying on a certificate will:

- Receive notice of the Cybertrust CA and associated conditions for relying parties.
- Validate a Cybertrust certificate by using certificate status information (e.g. a CRL or OCSP) published by Cybertrust, in accordance with the certificate path validation procedure, and validate at least those certificate attributes that materially affect the relying party's own signature policy if available.
- Trust a Cybertrust certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.

- Rely on a Cybertrust certificate only as it may be reasonable under the circumstances.
- Trust a certificate only if it has not been revoked.
- Validate at least those certificate attributes that materially affect the relying party's own policies or practices.

4.6.2.2Cybertrust CA Repository and Web site Conditions

Parties, including subscribers and relying parties, accessing the Cybertrust CA Repository and web site agree with the provisions of this CP and any other conditions of use that the Cybertrust CA may make available. Parties demonstrate acceptance of the conditions of usage of the CP by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. Using Cybertrust CA Repositories results includes:

- Obtaining information as a result of the search for a certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Obtaining information published on the Cybertrust CA web site.

4.7 Certificate Renewal

Renewal of Cybertrust certificates is not supported, all issued certificates must be replaced by certificates with a different public and private key pair upon expiration to bring effect to the Cybertrust policies that limit the useful life of a specific key pair.

4.8 Certificate Revocation and Suspension

The identification of the subscriber who applies for a revocation is carried out according to an internal procedure.

Subject to prior agreement with Cybertrust any Cybertrust RA may carry out the identification and authentication of holders seeking to revoke a certificate. Cybertrust enables Cybertrust RAs to rely on a shared secret presented by the subscriber at the time of end entity certificate enrolment as proof of identity and authenticity of the revocation request

Revocation requests can also be placed directly to the Cybertrust RA at: Cybertrust RA Office, Verizon Enterprise Solutions, Culliganlaan 2E, 1830, Diegem, Belgium or EVServiceDesk@verizonbusiness.com.

Upon request from an RA, the Cybertrust CA revokes the certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject. This is in effect even when Cybertrust or an external audit reveals suspicion of breach of a material obligation under this CP without timely resolution.
- The certificate's subject or their appointed subscriber has breached a material obligation under this CP or either the CA chaining agreement or applicable subscriber agreement.
- The performance of a person's obligations under this CP is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the

person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.

The Cybertrust RA requests the revocation of a certificate promptly upon verifying the identity of the requesting party and confirming that it has not been issued in accordance with the procedures required by this CP. Verification of the identity can be done through information elements featured in the identification data that the subscriber has submitted to the Cybertrust RA. Upon request by a Cybertrust RA, the Cybertrust CA takes prompt action to revoke the certificate.

Cybertrust does not provide certificate suspension services directly to subscribers. Cybertrust is allowed to suspend a certificate for up to 7 calendar days if subscriber does not fulfil its obligations including financial compensation. Subscriber will be informed of a suspension and its reasons.

4.9 Certificate Status Services

The Cybertrust CA makes available certificate status checking services including CRLs, OCSP where applicable, and appropriate web interfaces.

4.10 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

5. Management, Operational, And Physical Controls

This section describes non-technical security controls used by Cybertrust CA to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1 Physical Security Controls

The Cybertrust CA implements physical controls on its own leased or rented premises. Cybertrust requires physical controls by service providers that it may use to deliver its services.

The Cybertrust CA infrastructure is logically separated from other certificate management infrastructure, used for other purposes.

The Cybertrust CA secure premises are located in an area appropriate for high security operations.

Physical access is restricted by implementing multi-factor and multi-person authentication mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and

supported by security alarms and requiring movement from zone to zone to be accomplished using multiple tokens and access control lists.

The Cybertrust CA implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The Cybertrust CA implements a partial off-site backup.

The sites of the Cybertrust CA host the infrastructure to provide the Cybertrust CA services. The Cybertrust CA sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list, which is subject to audit.

5.2 Procedural Controls

The Cybertrust CA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The Cybertrust CA takes measures regarding confidentiality and protecting personal data.

All members of the staff operating as key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

Cybertrust may exercise vetting of personnel in trusted positions.

Cybertrust pursues the accountability of all actors for actions performed.

The Cybertrust CA implements multi-factor and multi-person control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The Cybertrust CA carries out checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Background checks include:

- Correlating facts provided by the candidate to publicly available information so as to detect misrepresentations by the candidate.
- Other checks as might be deemed necessary including, but not limited to, external background checks..

5.3.2 Training Requirements and Procedures

The Cybertrust CA makes available training for their personnel to carry out CA and RA functions.

5.3.3 Retraining Period and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.4 Sanctions against Personnel

Cybertrust CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.5 Controls of independent contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as Cybertrust CA personnel.

5.3.6 Documentation for initial training and retraining

The Cybertrust CA, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment. Cybertrust CA implements the following controls:

Cybertrust CA audit records events as they occur that include but are not limited to

- Issuance of a certificate
- Revocation of a certificate
- Published CRLs

Audit trail records contain:

- The identification of the operation
- The date and time of the operation
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents that are required for audits include:

- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

Cybertrust CA ensures that designated personnel review log files at regular intervals and detect and report anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of Cybertrust CA, the RA and designated auditors. The log files are properly protected by an access control mechanism. Log files and audit trails are backed up.

Auditing events are not specifically noted in the log being audited.

5.5 Records Archival

Cybertrust CA keeps internal records of the following items:

- CA certificates for a period of a maximum of 10 years after the expiration of the certificate.
- End entity certificates for a period of a maximum of 7 years after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of 7 years after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of 7 years after revocation of a certificate.
- CRLs for a minimum of 7 years after expiration or revocation of a certificate.
- Support documents on the issuance of certificates for a period of 7 years after expiration of a certificate.

Cybertrust CA keeps archives in a retrievable format.

5.5.1 Types of records

Cybertrust CA retains in a trustworthy manner records of Cybertrust CA digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

5.5.2 Retention period

Cybertrust CA retains in a trustworthy manner records of CA certificates for a maximum of 10 years following expiration or revocation.

5.5.3 Protection of archive

Conditions for the protection of archives include:
Only the records administrator (member of staff assigned with the records retention duty) may view the archive and is obligated to ensure:

- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

5.5.4 Procedures to obtain and verify archive information

To obtain and verify archive information, Cybertrust CA maintains records under clear hierarchical control and a definite job description.

Cybertrust CA retains records in electronic or in paper-based format. The Cybertrust CA may require RAs, subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic, in paper-based format or any other format that Cybertrust CA may see fit.

Cybertrust CA may revise record retention terms as it might be required in order to comply with accreditation requirements.

5.6 Compromise and Disaster Recovery

In a separate internal document, Cybertrust CA documents applicable incident, compromise reporting and handling procedures. Cybertrust CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

Cybertrust CA establishes the necessary measures to ensure recovery of the service in case of a disaster, corrupted servers, software or data.

5.7 CA or RA Termination

Before terminating its CA activities, the Cybertrust CA will take steps to transfer to a designated organisation the following information at the Cybertrust CA's own costs:

- All information, data, documents, repositories, archives and audit trails pertaining to Cybertrust CA.

6. Technical Security Controls

This section sets out the security measures taken by Cybertrust CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

6.1 Key Pair Generation and Installation

Cybertrust CA protects its private key(s) in accordance with this CP. For specific types of certificates Cybertrust CA uses private signing keys only for signing CRLs, and OCSP responses in accordance with the designated use of each of these keys.

Cybertrust CA will refrain from using its private keys used within Cybertrust CA in any way outside the scope of Cybertrust CA.

6.1.1 Cybertrust CA Private Key Generation Process

The Cybertrust CA uses a trustworthy process for the generation of its root private key according to a documented procedure. The Cybertrust CA distributes the fractional mirrors of its private key(s) across multiple high security facilities.

6.1.1.1Cybertrust CA Private Key Usage

The private keys of the Cybertrust CA are used to sign Cybertrust CA issued certificates, Cybertrust CA certification revocation lists and OCSP responses. Other usages are restricted.

6.1.1.2Cybertrust CA Private Key Type

For the CA Root key it uses, the Cybertrust CA makes use of the RSA or ECC algorithm with a key length of minimum 2048 bits (RSA) or minimum 256 bits (ECC) and a validity period of at least 20 years. Larger key sizes and longer validity periods may be used.

For the operational CA keys it uses the Cybertrust CA makes use of the RSA or ECC algorithm with a key length of 2048 bits (RSA) or minimum 256 bits (ECC) and a validity period of up to 14 years.

6.1.2 Cybertrust CA Key Generation

The Cybertrust CA securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of them. The Cybertrust CA implements and documents key generation procedures, in line with this CP.

The key generation is carried out using an algorithm recognized as being fit for the purposes of issuing certificates.

The selected key length and algorithm for CA signing key is recognized as being fit at the time for the purposes of issuing certificates as issued by the CA.

6.2 Key Pair re-generation and re-installation

The Cybertrust CA decommissions and destroys keys used in the past as well as the active tamper-resistant devices and all backup or escrowed copies of its private keys.

6.2.1 Cybertrust CA Key Generation Devices

The generation of the private keys of the Cybertrust CA occurs within a secure cryptographic hardware device.

6.2.1.1Cybertrust CA Key Generation Controls

The generation of the private key of the Cybertrust CA requires the control of more than one appropriately authorised member of staff serving in trustworthy positions. This action entails dual control.

6.2.2 Cybertrust CA Private Key Storage

The Cybertrust CA uses a secure cryptographic hardware device to store its private keys meeting the appropriate requirements of ISO and FIPS 140.

When outside the signature-creation device the Cybertrust private signing key for a certificate is encrypted at all times.

6.2.2.1Cybertrust CA Key Storage Controls

The storage of the private key of the Cybertrust CA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.2Cybertrust CA Key Back Up

The Cybertrust CA's private keys are split, backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.3Secret Sharing

The Cybertrust CA secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of private keys and provide for key recovery. The Cybertrust CA stores its own private keys in several tamper-resistant devices. This action entails dual control.

6.2.2.4Acceptance of Secret Shares

Before secret shareholders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody.

A secret shareholder receives the secret share within a physical medium, such as a Cybertrust CA approved cryptographic hardware module. The Cybertrust CA keeps written records of secret share distribution.

6.2.3 Cybertrust CA Public Key Distribution

Public key distribution of Cybertrust's own public key takes place according to Cybertrust's own practices as well as additional conditions required by law. Cybertrust CA Public Key and Certificates are made available to Subscribers and Relying Parties through their inclusion in web browser software. Cybertrust provides new root CAs to user agent (browser, etc) manufacturers for inclusion in browser and other software updates.

The Cybertrust CA documents its own private key distribution and has the ability to alter the distribution of tokens in case token custodians need to be replaced in their role as token custodians.

6.2.4 Cybertrust CA Private Key Destruction

Cybertrust CA private keys are destroyed by at least two trusted operatives present at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

Key destruction process is documented and associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

The Cybertrust CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements such as FIPS 140-2 level 3, which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted.

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

Cybertrust CA custodians are assigned with the task to activate and deactivate the private key. The key is then active for a defined time period.

The Cybertrust CA private keys can be destroyed at the end of their lifetimes.

6.4 Other Aspects of Key Pair Management

The Cybertrust CA archives its own public keys. The Cybertrust CA issues subscriber certificates with usage periods as indicated on such certificates.

6.4.1 Computing resources, software, and/or data are corrupted

The Cybertrust CA establishes the necessary measures to ensure full recovery of the service in case of a disaster, corrupted servers, software or data.

If resources or services are not retained under the control of the Cybertrust CA, the CA ensures that any agreement with the resource owner or services provider is compliant with the requirements for disaster recovery.

6.4.2 CA public key revocation

If a Cybertrust CA public key is revoked the Cybertrust CA will immediately:

- Notify all CAs with which it is cross-certified or has signed..

6.4.3 CA private key is compromised

If the private key of the Cybertrust CA is compromised, the corresponding certificate will immediately be revoked. Additional measures will be taken including the revocation of all end entity certificates.

6.5 Activation Data

The Cybertrust CA securely stores and archives activation data associated with its own private key and operations.

6.6 Computer Security Controls

The Cybertrust CA implements computer security controls.

6.7 Life Cycle Security Controls

The Cybertrust CA performs periodic development controls and security management controls.

6.8 Network Security Controls

The Cybertrust CA complies with the CA / Browser Forum Network and Certificate System Security Requirements, v. 1.0 as available at https://www.cabforum.org.

The Cybertrust CA maintains a high-level network of systems security including firewalls. Network intrusions are detected. Specifically:

- The Cybertrust CA encrypts connections to the RA, using dedicated administrative certificates.
- The Cybertrust CA website provides certificate based Secure Socket Layer connections and anti-virus protection.
- The Cybertrust CA network is protected by a managed firewall and intrusion detection system.
- Accessing Cybertrust CA databases from outside the CAs network is prohibited.
- Internet sessions for request and delivery of information are encrypted.

7. Certificate and CRL Profiles

This section specifies the certificate format, CRL and OCSP formats.

7.1 Certificate Profile

7.2 Cybertrust makes available the certificate profiles of the CA certificates it uses in its CP upon receiving a duly justified request. CRL Profile

The Cybertrust CA maintains a record of the CRL profile it uses in an independent technical document. This will be made available at the discretion of the Cybertrust CA, on request from parties explaining their interest.

In conformance with IETF PKIX RFC 2459, 3280 and 5280 Cybertrust supports CRLs compliant with:

- Version numbers supported for CRLs; and
- CRL and CRL entry extensions populated and their criticality.

The profile of the Cybertrust Certificate Revocation List is showing in the table below:

Version	[Version 2]	
Issuer Name	CountryName=[Root Certificate Country Name], organizationName=[Root Certificate Organisation], commonName=[Root Certificate Common Name] [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + CRL Usage Period]	
Revoked Certificates	*CRL Entries*	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

7.3 OCSP Profile

The Cybertrust CA maintains a record of the OCSP profile it might use in an independent technical document. This will be made available at the discretion of the Cybertrust CA, on request from parties explaining their interest.

8. Compliance Audit and Other Assessment

The Cybertrust CA accepts under condition the auditing of practices and procedures it does not publicly disclose. The Cybertrust CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content the Cybertrust CA accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CP and accreditation schemes it publicly claims compliance with.

8.1 Compliance Audit and Other Assessment

Information on Cybertrust's conformance with the requirements of any accreditation scheme can be sought by the organization of such accreditation scheme directly.

Cybertrust has successfully been audited and currently meets the requirements of the accreditation scheme known as WebTrust for Certification Authorities including the Extended Validation and SSL Baseline Requirements audits. Cybertrust seeks to maintain its accreditation.

Cybertrust accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CP. Cybertrust accepts this auditing of its own practices and procedures that it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by a party to which Cybertrust owes duty.

The CA evaluates the results of such audits before further implementing them.

8.1.1 Audit process conditions

To carry out the audits, there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with Cybertrust nor having any conflicting interests thereof.

An audit is carried out in areas that include but are not limited to the following ones:

- Compliance of Cybertrust operating procedures and principles with the procedures and service levels defined in the CP.
- Compliance of Omniroot subscribers with this CP.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CP.
- Adherence to relevant laws.
- Asserting agreed service levels.
- Inspection of audit trials, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

With regard to conformance audits, Cybertrust undertakes the responsibility of the performance of any subcontractors it uses to carry out certification operations including those described in the section below.

8.1.1.1 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, Cybertrust may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. Cybertrust may outsource in part or whole certain aspects of the delivery of its services. Regardless of the partner or agent selected to manage certain parts of the certificate life cycle or operations, Cybertrust remains ultimately in charge of the whole process. Cybertrust limits its responsibility thereof according to the conditions in this Cybertrust CP.

8.1.1.2 Secure Devices and Private Key Protection.

Cybertrust supports the use of secure devices and tamperproof equipment to securely issue, manage and store certificates. Cybertrust uses accredited trustworthy hardware to prevent compromise of its private key.

9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of the Cybertrust CA certificates under this CP as described in this section.

9.1 Fees

The issuance and management of Cybertrust CA and end entity certificates is subject to fees which can be quoted on request.

9.1.1 Refund policy

Refund requests must be duly justified and addressed to the Legal Services of Cybertrust. Cybertrust reserves its right to endorse or grant and refunds unless they are requested in the framework of a warranty offered by Cybertrust.

9.2 Financial Responsibility

Cybertrust maintains sufficient resources to meet its perceived obligations under this CP. The Cybertrust CA makes this service available on an “as is” basis.

9.3 Confidentiality of Business Information

The Cybertrust CA observes personal data privacy rules and confidentiality rules as described in the Cybertrust CP. Confidential information includes:

- Any personal identifiable information about subscribers, other than that contained in a certificate.
- Reason for the revocation of a CA certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificates and their content.
- Status of a certificate.

Cybertrust does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the Cybertrust CA owes a duty to keep information confidential is the party requesting such information.
- A court order.

The Cybertrust CA may charge an administrative fee to process such disclosures.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- Only a single certificate is delivered per inquiry by subscriber or relying party.
- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to subscribers nor relying parties. The Cybertrust CA properly manages the disclosure of information to the CA personnel.

The Cybertrust CA authenticates itself to any party requesting the disclosure of information by:

- Presenting an authentication certificate at the request of the subscriber or relying party
- Signing responses to OCSP requests and CRLs.

The Cybertrust CA encrypts all communications of confidential information including:

- The communications link between the CA and the RAs.
- Sessions to deliver certificates and certificate status information.

To incorporate information by reference the Cybertrust CA uses computer-based and text-based pointers that include URLs, etc.

9.4 Privacy of Personal Information

Cybertrust CA makes available a specific Data Protection Policy for the protection of personal data of the applicant applying for a Cybertrust CA certificate that they make available through their web site. The Cybertrust CA adheres to the documented Privacy Policy of Cybertrust available from https://secure.omniroot.com/repository .

9.5 Intellectual Property Rights

Cybertrust owns and reserves all intellectual property rights associated with its databases, web sites, Cybertrust CA digital certificates and any other publication whatsoever originating from Cybertrust CA including this CP.

The distinguished names of all CAs of Cybertrust CA, remain the sole property of Cybertrust, which enforces these rights.

Certificates are and remain property of the Cybertrust CA or the rightful owner that licenses certificate management over to Cybertrust. The Cybertrust CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of the Cybertrust CA. The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.

The Cybertrust CA owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Representations and Warranties

The Cybertrust CA uses this CP and a subscriber agreement to convey legal conditions of usage of Cybertrust CA certificates to subscribers and relying parties.

Participants that may make certain (limited) representations include Cybertrust CA, RAs, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the Cybertrust domain, including the Cybertrust CA, RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

9.6.1 Subscriber Obligations

Unless otherwise stated in this CP, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with the Cybertrust CA.
- Ensuring that the public key submitted to the Cybertrust CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the Cybertrust CA CP and associated policies published in the Cybertrust CA Repository.
- Refraining from tampering with a Cybertrust CA or end entity certificate.
- Using Cybertrust certificates for legal and authorised purposes in accordance with this CP.
- Notifying Cybertrust CA or a Cybertrust RA of any changes in the information submitted.
- Ceasing to use a Cybertrust certificate if any featured information becomes invalid.
- Ceasing to use a Cybertrust certificate when it becomes invalid.
- Removing a Cybertrust certificate when invalid from any applications and/or devices they have been installed on.
- Using a Cybertrust certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- For any acts and omissions of partners and agents that subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting to Cybertrust CA or any Cybertrust CA directory any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a Cybertrust certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.
- Submitting accurate and complete information to Cybertrust in accordance with the requirements of this CP particularly with regards to registration.
- Only using the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber according to this CP or either the executed CA Chaining agreement or applicable subscriber agreement.

- Exercising absolute care to avoid unauthorized use of its private key.
- Generating subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures;
- Using a key length and algorithm which is recognized as being fit for the purposes of electronic signatures.
- Notifying Cybertrust without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The subscriber's private key has been lost, stolen, potentially compromised; or
    - Control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code)
      or
    - Inaccuracy or changes to the certificate content, as notified to the subscriber.

The subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and Cybertrust must designate the usage of a trustworthy device as well as the choice of organizational context.

As a root authority and operator of a trust network that makes available a unique and critical service, Cybertrust seeks to ensure the trustworthiness of the relationship with the CA chaining and end entity subscriber.

9.6.2 Relying Party Obligations

A party relying on a Cybertrust certificate promises to:

- Have the technical capability to use digital certificates.
- Receive notice of the Cybertrust CA and associated conditions for relying parties.
- Validate a Cybertrust certificate by using certificate status information (e.g. a CRL) published by the Cybertrust CA in accordance with the proper certificate path validation procedure.
- Trust a Cybertrust certificate only if all information featured on such certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a Cybertrust certificate, only as it may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised.

The obligations of the relying party, if it is to reasonably rely on a certificate, are to:

- Verify the validity or revocation of the certificate using current revocation status information as indicated to the relying party.
- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or this CP.
- Take any other precautions prescribed in the Cybertrust certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

Relying parties must at all times establish that it is reasonable to rely on a certificate under the circumstances taking into account circumstances such as the specific application context a certificate is used in.

9.6.2.1 Conveying Relying party obligations

In order to give uninhibited access to revocation information and subsequently invoke trust in its own services, Cybertrust refrains from implementing an agreement with the relying party with regard to controlling the validity of certificate services with the purpose of binding relying parties to their obligations.

Much like it applies to any other participant of Cybertrust public services, however, the use of Cybertrust resources that relying parties make is implicitly governed by the conditions set out in Cybertrust's policy framework instantiated by the Cybertrust CP.

Relying parties are hereby notified that the conditions prevailing in this CP are binding upon them each time they consult a Cybertrust resource for the purpose of establishing trust and validating a certificate.

9.6.3 Subscriber Liability towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CP, subscribers are liable for any misrepresentations they make in certificates to third parties that, reasonably rely on the representations contained therein.

9.6.4 Cybertrust CA Repository and Web site Conditions

Parties (including subscribers and relying parties) accessing the Cybertrust CA Repository and web site agree with the provisions of this CP and any other conditions of usage that Cybertrust may make available. Parties demonstrate acceptance of the conditions of usage of the CP by submitting a query with regard to the status of a certificate or by anyway using or relying upon any such information or services provided. The Cybertrust CA Repositories include or contain:

- Information provided as a result of the search for a certificate.
- Information to verify the status of digital signatures created with a private key corresponding to a public key listed in a certificate.
- Information to verify the status of a digital certificate before encrypting data using the public key included in a certificate
- Information published on the Cybertrust CA web site.
- Any other services that Cybertrust CA might advertise or provide through its web site.

The Cybertrust CA maintains a certificate repository during the application period and for 5 years after the expiration or revocation of a certificate. To verify its integrity the complete repository will be made available to the Cybertrust RAs for queries at any time.

Additionally, the Cybertrust CA repository is available to relying parties.

9.6.4.1Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the Cybertrust CA Repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The Cybertrust CA takes all steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the Cybertrust Repositories and web site may result in terminating the relationship between the Cybertrust CA and the party.

9.6.4.2Accuracy of Information

The Cybertrust CA makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information. The Cybertrust CA, however, cannot accept any liability beyond the limits set in this CP.

9.6.5 Cybertrust CA Obligations

To the extent specified in the relevant sections of the CP, the Cybertrust CA promises to:

- Comply with this CP and its amendments as published under https://secure.omniroot.com/repository.
- Manage and operate the service to be compliant to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, the Guidelines for Extended Validation Certificates, and the CA / Browser Forum Network and Certificate System Security Requirements, v. 1.0 as available at https://www.cabforum.org.
- Provide infrastructure and certification services, including the establishment and operation of the Cybertrust CA Repository and web site for the operation of public certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available.
- Issue electronic certificates in accordance with this CP and fulfil its obligations presented herein.
- Revoke certificates issued according to this CP upon receipt of a valid and authenticated request to revoke a certificate from an RA.
- Publish accepted certificates in accordance with this CP.
- Provide support to subscribers and relying parties as described in this CP.
- Provide for the expiration and re-keying of certificates according to this CP.
- Publish CRLs and/or OCSP responses of all suspended and revoked certificates on a regular basis in accordance with this CP.
- Provide appropriate service levels according to a service agreement.
- Notify relying parties of certificate revocation by publishing CRLs on the Cybertrust CA repository.

Cybertrust might seek additional insurance coverage against risks emanating from the correctness of the information included in a certificate.

To the extent permitted by law the Cybertrust CA cannot be held liable for:

- Any use of certificates, other than specified in this CP.
- Falsification of transactions.
- Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving certificates.
- Compromise of private keys associated with the certificates.
- Loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates.
- The submission of erroneous or incomplete data from an RA, including identification data, serial numbers and public key values.
- Erroneous or incomplete requests for operations on certificates by the RA.

- Acts of God.
- The use of certificates.
- The use of public or private keys of cross-certified (non-subordinate) CA's and their relying parties.
- Services delivered to any subscriber that maintains a CA chaining relationship within its own organisation with another certification authority. This limitation applies to the services delivered to the whole customer organisation and not just specific root or roots that the customer has CA chained.

The Cybertrust CA acknowledges it has no further obligations under this CP.

9.6.6 Registration Authority Obligations

A Cybertrust RA operating within the Cybertrust network promises to:

- Generate securely an RA administrator key pair, using a trustworthy system directly or through an agent.
- Provide correct and accurate information in their communications with the Cybertrust CA.
- Ensure that the public key submitted to Cybertrust CA is the correct one (if applicable).
- Generating a new, secure key pair to be used in association with a certificate that they request from Cybertrust CA.
- Receive applications for the Cybertrust CA certificates in accordance with this Cybertrust CP.
- Carry out all verification and authenticity actions prescribed by the Cybertrust CA procedures and this CP.
- Submit to the Cybertrust CA the applicant's request in a signed message (certificate request).
- Receive, verify and relay to the Cybertrust CA all requests for revocation of a Cybertrust CA certificate in accordance with the Cybertrust CA procedures and the Cybertrust CA CP.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of future repetitive issuance in response to expiration of a certificate according to this CP.

9.6.7 Information incorporated by reference into a digital certificate

The Cybertrust incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the corresponding CP.
- Any other applicable certificate policy as may be stated on an issued Cybertrust certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customised elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

9.6.8 Pointers to incorporate by reference

To incorporate information by reference Cybertrust uses computer-based and text-based pointers. Cybertrust may use URLs, OIDs etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

The Cybertrust CA does not warrant:

- The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CP and in the Cybertrust CA warranty policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in free, test or demo certificates.

9.7.2 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) is the Cybertrust CA liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CP.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

9.8 Limitations of Liability

The total liability of the Cybertrust CA is limited in accordance with the provisions of the applicable agreement.

Further information can be found at:
https://secure.omniroot.com/repository.

9.9 Indemnities

This section contains the applicable indemnities.

9.9.1 Indemnity

To the extent permitted by law the subscriber agrees to indemnify and hold the Cybertrust CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that the Cybertrust may incur as a result of:

- Failure to protect the subscriber's private key,
- Failure to use a trustworthy system as required, or
- Failure to take precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key

9.10 Term and Termination

This CP remains in force until notice of the opposite is communicated by the Cybertrust CA on its web site or repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.11 Individual notices and communications with participants

The Cybertrust CA accepts notices related to this CP by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Cybertrust CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individual communications made to the Cybertrust CA must be addressed to: EVServiceDesk@verizonbusiness.com or by post to the Cybertrust in the address mentioned in the introduction of this document.

9.12 Amendments

Changes to this CP are indicated by appropriate numbering.

The Cybertrust CA Policy Management Authority decides on the numbering of versions.

9.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify Cybertrust of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, Cybertrust convenes a Dispute Committee that advises Cybertrust management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a data protection officer, a member of Cybertrust operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to the Cybertrust executive management. The Cybertrust executive management may subsequently communicate the proposed settlement to the resting party.

9.13.1 Arbitration

If the dispute is not resolved within twenty (20) days after initial notice pursuant to CP, parties submit the dispute to arbitration, in accordance with Article 1676-1723 of the Belgian Judicial Code.

There will be 3 arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Leuven, Belgium and the arbitrators determine all associated costs.

For all technology related disputes and disputes related to this CP the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes)

9.14 Governing Law

This CP is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Cybertrust digital certificates or other products and services. The laws of Belgium apply also to all Cybertrust commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to Cybertrust products and services where the Cybertrust acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including Cybertrust partners, subscribers and relying parties, irrevocably submit to the jurisdiction of the district courts of Belgium.

9.15 Compliance with Applicable Law

Cybertrust CA complies with applicable laws of Belgium. Export of certain types of software used in certain Cybertrust CA public certificate management products and services may require the approval of appropriate public or private authorities. Parties (including the Cybertrust CA, subscribers and relying parties) agree to conform to applicable export laws and regulations as pertaining in Belgium.

Cybertrust CA operates within the trade restrictions of the US Bureau of Industry and Security within the US Department of Commerce.

9.16 Miscellaneous Provisions

9.16.1 Survival

The obligations and restrictions contained under section “Legal Conditions” survive the termination of this CP.

9.16.2 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CP will be interpreted in such manner as to effect the original intention of the parties.

10. List of definitions

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.
ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.
APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to a CA to issue a digital certificate.
ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.
ASSURANCES
A set of statements or conduct aiming at conveying a general intention.
AUDIT
Procedure used to validate compliance with formal criteria or controls.
AUTHENTICATED RECORD
A signed document containing assurances of authentication or a message with a digital signature verified by a valid certificate by a relying party.
AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and veryfying such relationship.
AUTHORISATION
Granting of rights.
AVAILABILITY
The rate of accessibility of information or resources.
HARDWARE MODULE
The complete system of the hardware module used to keep the certificates and securely generate a key pair.
BINDING
A statement by an RA of the relationship between a named entity and its public key.
CERTIFICATE
The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's ones .
CERTIFICATE REVOCATION LIST OR **CRL**
A list maintained by the CA of certificates that are revoked before their expiration time.
CERTIFICATION AUTHORITY OR **CA**
An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the Cybertrust CA.
CERTIFICATION PRACTICE STATEMENT OR **CPS**
A statement of the practices in the management of certificates during all life phases.
CERTIFICATE STATUS SERVICE OR **CSS**
A service, enabling relying parties and others to verify the status of certificates.
CONTRACT PERIOD
The duration of the Cybertrust CA contract between the Applicant and the CA organization.
CERTIFICATE CHAIN
A hierarchical list certificates containing an end-user subscriber certificate and CA certificates.
CERTIFICATE EXPIRATION
The end of the validity period of a digital certificate.
CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.
CERTIFICATE HIERARCHY
A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.
CERTIFICATE MANAGEMENT
Actions associated with certificate management include, storage, dissemination, publication, revocation, and suspension of certificates.
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to me consulted by relying parties at all times prior to relying on information featured in a certificate.
CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA.
CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital certificate.
CERTIFICATION

The process to issue a digital certificate.

CERTIFICATION AUTHORITY (CA)
An authority, such as the Cybertrust CA that issues, suspends, or revokes a digital certificate.

CERTIFICATE POLICY (CP)
A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a certificate. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with RFC 3647 and RFC 3039

CERTIFICATE SUSPENSION
Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

CERTIFICATE REVOCATION
Online service used to permanently disable a digital certificate before its expiration date

CERTIFICATE REVOCATION LISTS
Online publication of complete and incremental digital certificates revocation lists compliant with RFC 2459

COMMERCIAL REASONABLENESS
A legal term from Common Law. In electronic commerce it means the usage of technology that provides reasonable assurance of trustworthiness.

COMPROMISE
A violation of a security policy that results in loss of control over sensitive information.

CONFIDENTIALITY
The condition to disclose data to selected and authorised parties only.

CONFIRM A CERTIFICATE CHAIN
To validate a certificate chain in order to validate an end-user subscriber certificate.

DIGITAL CERTIFICATE
A formatted piece of data that relates an identified subjext with a public key the subject uses.

DIGITAL SIGNATURE
To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.

DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE
Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

END-USER SUBSCRIBER
A subscriber other than another CA.

ENHANCED NAMING
The usage of an extended organisation field (OU=) in an X.509 v.3.0 certificate.

EXTENSIONS
Extension fields in X.509 v.3.0 certificates.

GENERATE A KEY PAIR
A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HASH
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION
The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

INCORPORATE BY REFERENCE
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

KEY GENERATION PROCESS
The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

KEY PAIR
A private key and its corresponding public key in asymmetric encryption.

NOTICE
The result of notification to parties involved in receiving CA services in accordance with this CP.
NOTIFY
To communicate specific information to another person as required by this CP and applicable law.
NOTARISED TIME STAMPING
Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis with up-to-date technology.
OBJECT IDENTIFIER
A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.
PKI HIERARCHY
A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.
PRIVATE KEY
A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.
PUBLIC KEY
A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.
PUBLIC KEY CRYPTOGRAPHY
Cryptography that uses a key pair of mathematically related cryptographic keys.
PUBLIC KEY INFRASTRUCTURE (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.
REGISTRATION AUTHORITY OR **RA**:
An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.
RELATIVE DISTINGUISHED NAME (RDN)
A set of attributes that distinguishes the entity from others of the same type.
RELIANCE
To accept a digital signature and act in a way that shows trust in it.
RELYING PARTY
Any entity that relies on a certificate for carrying out any action.
REPOSITORY
A database and/or directory listing digital certificates and other relevant information accessible on-line.
REVOKE A CERTIFICATE
To permanently end the operational period of a certificate from a specified time forward.
SECRET SHARE
A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.
SECRET SHARE HOLDER
An person that holds a secret share.
SHORT MESSAGE SERVICE (SMS)
A service for sending messages to mobile phones.
SIGNATURE
A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.
SIGNER
A person who creates a digital signature for a message, or a signature for a document.
SMART CARD
A hardware token that contains a chip to implement among others cryptographic functions.
STATUS VERIFICATION
Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs
SUBJECT OF A DIGITAL CERTIFICATE
The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.
SUBSCRIBER
The subject of a digital certificate, or a party designated by the subject to apply for the certificate.
SUBSCRIBER AGREEMENT
The agreement between a subscriber and a CA for the provision of public certification services.
SUSPENDED CERTIFICATE
Temporarily discarded certificate, which nevertheless is kept on hold for one week until revocation or reactivation notice is given to Cybertrust CA by the RA.
TRUSTED POSITION

A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

CYBERTRUST CA REGISTRATION AUTHORITY:

An entity that verifies and provides all subscriber data to the Cybertrust CA.

CYBERTRUST CA PUBLIC CERTIFICATION SERVICES

A digital certification system made available by Cybertrust CA as well as the entities that belong to the Cybertrust CA domain as described in this CP.

CYBERTRUST CA PROCEDURES

A document describing the Cybertrust CA's internal procedures with regard to registration of end users, security etc.

WEB -- WORLD WIDE WEB (WWW)

A graphics based medium for the document publication and retrieval of information on the Internet.

WRITING

Information accessible and usable for reference.

X.509

The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

11. List of acronyms

CA: Certification Authority
CEN/ISSS: European Standardisation Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
CYBERTRUST CA: Cybertrust Certification Authority
IETF: Internet Engineering Task Force
ISO: International Standards Organisation
ITU: International Telecommunications Union
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax