Cybertrust CA Certificate Policy

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V 2.4	22.07.13	Steven Medin	Align with CPS v5.5 (Unpublished)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:

-

1. Introduction

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 bes lp

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

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

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.

- 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

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.

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-

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.

Xti 24.13138s4(h)0.685979(e)0.685979( )-11.729ea Poll nnts lrsot1-5.01627( )-11.7302(i)4.70385(n)0.686716(t)0.341

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 e (o)0.686716(t)0.341884(i)3.70178(s)-7.026394t204i.88.3853(e)0.6862(i)4.70385a[(n)0.686ecte su(o)0.686716i0 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 Cybpito p84(u)11.38.686716(t)0.341884(i)-7.368239(n868(e)0.68e)0.685979(r)

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 c

- 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.
-

- 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

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 intermediat

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 onairssfena.6.1 ons oir16( )0.341884(t)0.2t6(r)-5.016s e884(t
2631( )-11.7287( )0.685242( )-11.7287(o)0.685242(f)-11.3853(n)0.341884(t)0.341884(h)-11.3853(e)l borelosn1 1(t)9996 T(s)-7.02631s

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

- 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 Cybedure. er whoei

[redacted]

[redacted]

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, au.683768(u n.1m9)1384

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

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

[redacted]

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. e

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). I

- 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

[redacted]

- 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.

9.7 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:

-

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 ur0388q85(,)-11.705(p)016(r)-5.01627(.)0.341860.686716(t)0.341884(e)0.686716(

[redacted]

10. List of definitions

ACCEPT (

[redacted]

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

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 Institu