

Certification Practice Statement



Certification Practice Statement

for Cybertrust Certification Services

Date: September 22, 2008

Version: v.5.4

Cybertrust Certification Practice Statement

Table of Contents

Document History	1
Acknowledgments	4
1. Introduction.....	5
1.1 Overview	5
1.2 Cybertrust Certificate types.....	7
1.2.1 Personal Certificates.....	7
1.2.2 Server Certificates	7
1.2.3 Object Publishing Certificates	7
1.2.4 Acceptable Subscriber Names	7
1.2.5 Registration procedures.....	8
1.3 SureCredential Demo and SureCredential 1.....	8
1.3.1 General	8
1.3.2 Assurance level	8
1.3.3 Individuals	8
1.3.4 Content.....	8
1.3.5 Submitted documents to identify the applicant.....	8
1.3.6 Time to confirm submitted data.....	8
1.3.7 Issuing procedure	8
1.3.8 Limited Warranty	8
1.3.9 Relevant Cybertrust Legal Documents	8
1.4 SureCredential Personal.....	8
1.4.1 General	8
1.4.2 Assurance Level	8
1.4.3 Individuals:	8
1.4.4 Content.....	9
1.4.5 Documents Submitted to Identify the Applicant	9
1.4.6 Time to Confirm Submitted Data	9
1.4.7 Issuing Procedure.....	9
1.4.8 Limited Warranty	10
1.4.9 Relevant Cybertrust Documents.....	10
1.5 SureCredential Professional	10
1.5.1 General	10
1.5.2 Individuals	11
1.5.3 Content.....	11
1.5.4 Documents Submitted to Identify the Applicant	11
1.5.5 Time to Confirm Submitted Data	12
1.5.6 Issuing Procedure.....	12
1.5.7 Limited Warranty	12
1.5.8 Relevant Cybertrust Documents.....	12
1.6 SureCredential 3.....	13
1.6.1 General	13
1.6.2 Individuals:	13
1.6.3 Content.....	13
1.6.4 Documents Submitted to Identify the Applicant	13
1.6.5 Time to Confirm Submitted Data	13
1.6.6 Issuing Procedure.....	13
1.6.7 Limited Warranty	13
1.6.8 Relevant Cybertrust Documents.....	13
1.7 SureCredential 3 Pro	13

Cybertrust Certification Practice Statement

1.7.1	General	13
1.7.2	Individuals	13
1.7.3	Content.....	13
1.7.4	Documents Submitted to Identify the Applicant	13
1.7.5	Time to Confirm Submitted Data	13
1.7.6	Issuing Procedure.....	13
1.7.7	Limited Warranty	13
1.7.8	Relevant Cybertrust Documents.....	13
1.8	SureServer	13
1.8.1	General	13
1.8.2	Business Entities	13
1.8.3	Content.....	13
1.8.4	Certificate Profile	14
1.8.5	Documents Submitted to Identify the Applicant	14
1.8.6	Time to Confirm Submitted Data	14
1.8.7	Issuing Procedure.....	14
1.8.8	Limited Warranty	14
1.8.9	Relevant Cybertrust Documents.....	14
1.9	SureServer EV.....	15
1.9.1	General	15
1.9.2	Business Entities	16
1.9.3	Content.....	16
1.9.4	Information Submitted to Identify the Applicant.....	17
1.9.5	Data Verification	17
1.9.6	Issuing Procedure.....	18
1.9.7	Limited Warranty	19
1.9.8	Insurance Plan.....	20
1.9.9	Relevant Cybertrust Documents.....	20
1.10	SureServer EDU.....	20
1.10.1	General	20
1.10.2	Business Entities	20
1.10.3	Content.....	21
1.10.4	Information Submitted to Identify the Applicant.....	21
1.10.5	Time to Confirm Submitted Data	21
1.10.6	Issuing Procedure.....	21
1.10.7	Limited Warranty	22
1.10.8	Relevant Cybertrust Documents.....	22
1.11	SureCodesign.....	22
1.11.1	General	22
1.11.2	Business Entities	22
1.11.3	Content.....	23
1.11.4	Documents Submitted to Identify the Applicant	23
1.11.5	Time to Confirm Submitted Data	23
1.11.6	Issuing Procedure.....	23
1.11.7	Limited Warranty	23
1.11.8	Relevant Cybertrust Legal Documents	24
1.12	Certificate usages	24
1.13	Document Name and Identification	25
1.14	PKI participants	25
1.14.1	Cybertrust Certification Authority.....	25
1.14.2	Cybertrust Registration Authorities.....	26
1.14.3	Subscribers	27

Cybertrust Certification Practice Statement

1.14.4	Subjects	28
1.14.5	Certificate Applicants	29
1.14.6	Relying Parties	29
1.15	Certificate use.....	29
1.15.1	Appropriate certificate usage.....	29
1.15.2	Prohibited certificate usage	29
1.15.3	Certificate extensions.....	29
1.15.4	Critical Extensions	30
1.16	Policy Administration	30
1.16.1	Scope	30
1.16.2	Cybertrust Policy Management Authority.....	30
1.16.3	Acceptance of Updated Versions of the CPS	31
1.16.4	Version management and denoting changes.....	31
1.17	Definitions and acronyms.....	31
2.	Publication and Repository Responsibilities	32
2.1	Access control on repositories	32
3.	Identification and Authentication	33
3.1	Naming.....	33
3.2	Initial Identity Validation	33
3.3	Subscriber registration process.....	34
3.3.1	Documents used for subscriber registration.....	34
3.3.2	Data needed for subscriber registration.....	36
3.3.3	Pseudonyms.....	36
3.3.4	Records for subscriber registration.....	37
3.4	Identification and Authentication for Revocation Requests.....	37
4.	Certificate Life-Cycle Operational Requirements	38
4.1	Certificate Application	38
4.2	Certificate Application Processing	38
4.3	Certificate Issuance	39
4.4	Certificate generation.....	39
4.5	Certificate Acceptance	39
4.6	Key Pair and Certificate Usage	40
4.6.1	Subscriber	40
4.6.2	Relying party	41
4.7	Certificate Renewal.....	42
4.8	Certificate Revocation and Suspension	42
4.8.1	Term and Termination of Suspension and Revocation.....	43
4.9	Certificate Status Services	43
4.10	End of Subscription.....	43
4.11	Certificates Problem Reporting and Response Capability	43
5.	Management, Operational, And Physical Controls.....	44
5.1	Physical Security Controls	44
5.2	Procedural Controls	44
5.3	Personnel Security Controls.....	45
5.3.1	Qualifications, Experience, Clearances	45
5.3.2	Background Checks and Clearance Procedures	45
5.3.3	Training Requirements and Procedures	45
5.3.4	Retraining Period and Retraining Procedures.....	45
5.3.5	Job Rotation	45
5.3.6	Sanctions against Personnel.....	45
5.3.7	Controls of independent contractors.....	46
5.3.8	Documentation for initial training and retraining.....	46

Cybertrust Certification Practice Statement

5.4	Audit Logging Procedures.....	46
5.5	Records Archival	46
5.5.1	Types of records.....	47
5.5.2	Retention period	47
5.5.3	Protection of archive	47
5.5.4	Archive Collection.....	47
5.5.5	Procedures to obtain and verify archive information	48
5.6	Compromise and Disaster Recovery	48
6.	Technical Security Controls	49
6.1	Key Pair Generation and Installation	49
6.1.1	Cybertrust CA Private Key Generation Process.....	49
6.1.2	Cybertrust CA Key Generation.....	49
6.1.3	Cybertrust Key Generation Audit (EV Guidelines)	50
6.2	Key Pair re-generation and re-installation.....	50
6.2.1	Cybertrust CA Key Generation Devices.....	50
6.2.2	Cybertrust CA Private Key Storage	50
6.2.3	Cybertrust CA Public Key Distribution	51
6.2.4	Cybertrust CA Private Key Destruction.....	51
6.3	Private Key Protection and Cryptographic Module Engineering Controls	51
6.4	Other Aspects of Key Pair Management.....	52
6.4.1	Computing resources, software, and/or data are corrupted.....	52
6.4.2	CA public key revocation.....	52
6.4.3	CA private key is compromised	52
6.5	Activation Data	52
6.6	Computer Security Controls	52
6.7	Life Cycle Security Controls	52
6.8	Network Security Controls.....	52
6.9	Time-stamping.....	53
7.	Certificate and CRL Profiles.....	54
7.1	Certificate Profile	54
7.2	CRL Profile	54
7.3	OCSP Profile	54
8.	Compliance Audit And Other Assessment	55
8.1	Compliance Audit And Other Assessment	55
8.1.1	Audit process conditions	55
9.	Other Business and Legal Matters	57
9.1	Fees	57
9.1.1	Refund policy.....	57
9.2	Financial Responsibility	57
9.3	Confidentiality of Business Information.....	57
9.3.1	Disclosure Conditions	58
9.4	Privacy of Personal Information	58
9.5	Intellectual Property Rights	58
9.6	Representations and Warranties	58
9.6.1	Relying Party Obligations.....	59
9.6.2	Subscriber Liability towards Relying Parties	60
9.6.3	Cybertrust CA Repository and Web site Conditions.....	60
9.6.4	Cybertrust CA Obligations.....	61
9.6.5	Registration Authority Obligations	62
9.6.6	Information incorporated by reference into a digital certificate	62
9.6.7	Pointers to incorporate by reference.....	62
9.7	Disclaimers of Warranties	63

Cybertrust Certification Practice Statement

9.7.1	Limitation for Other Warranties	63
9.7.2	Exclusion of Certain Elements of Damages.....	63
9.8	Limitations of Liability.....	63
9.8.1	Limitations on SureServer EV Certificate Liability	63
9.9	Indemnities.....	64
9.10	Term and Termination.....	64
9.11	Individual notices and communications with participants	65
9.12	Amendments	65
9.13	Dispute Resolution Procedures.....	65
9.13.1	Arbitration.....	65
9.14	Governing Law	65
9.15	Compliance with Applicable Law	66
9.16	Miscellaneous Provisions.....	66
9.16.1	Survival	66
9.16.2	Severability.....	66
10.	List of definitions.....	67
11.	List of acronyms	71

Copyright

Copyright © 2006 Cybertrust Holdings, Inc. and/or its affiliates and licensors. All rights reserved. No part of this publication may be copied or reproduced, stored in a retrieval system, sold or transferred to any person, in whole or in part, in any manner or form or on any media, without the prior written permission of Cybertrust.

Intellectual Property Rights

Any rights, including title, ownership rights, copyright, trademarks, patents and any other intellectual property rights of whatever nature, in this document and the services or products described herein, including any associated processes or any derivative works, will remain the sole and exclusive property of Cybertrust and/or its licensors and suppliers.

Disclaimer

Cybertrust has made all reasonable efforts to ensure that this publication is accurate. However, Cybertrust assumes no liability for any accidental error or omission that may be found in this publication. The information in this document is the latest available at its publication date. It may change over time; make sure that you use the latest version available of this publication.

Trademarks

Cybertrust and all names used to identify the products and/or services of Cybertrust in this documents are trademarks or registered trademarks of Cybertrust Holdings, Inc. and/or its affiliates and licensors. All other trademarks or registered trademarks that appear in this document are the property of their respective owners.

Cybertrust Certification Practice Statement

Document History

Document Change Control

Version	Release Date	Author	Status / Description
v5.0	10-JUL-2005	Andreas Mitrakas	Draft
	30-AUG-2005	Jean-Paul Declerck	Final version
	02-FEB-2006	Johan Sys	Administrative clean-up
v5.1	13-MAR-2006	Johan Sys	Added SureServer EDU
v5.2	29-NOV-2006	Philippe Deltombe	Added SureServer EV
	06-DEC-2006	Johan Sys	Removed HyperSign and ServerSign
v5.3	04-JUN-2007	Johan Sys	Administrative Update
	18-JUL-2007	Jean-Paul Declerck	General update / Removed certain policy references
V5.4	01-AUG-2008	Steven Medin	Administrative Update, SureCredential process steps and brand name accuracy

Cybertrust Certification Practice Statement

Summary of Changes

Changes in v5.4 (publication date : August 2008) with respect to v5.3

- Administrative Changes
- SureCredential product renaming
- SureCredential process update

Changes in v.5.3 (publication date: September 2007) with respect to v.5.2

- Administrative changes
- General update
- Language updates
- Removed certain outdated policy references and associated language.

Changes in v.5.2 (publication date: December 2006) with respect to v.5.1

- Added SureServer EV product
- Removed HyperSign and ServerSign products
- Administrative changes

Changes in v.5.1 (Publication Date: 13 March 2006) with respect to v.5.0

- Added SureServer EDU product

Changes in v.5.0 (Publication Date: 10 July 2005) with respect to v.4.3.2

- Adaptation to the RFC 3647 format
- Separation of Data protection policy, warranty policy and consumer policy.
- Updated references to Cybertrust Certificate Policy

Changes in v.4.3.2 (Publication Date: 8 April 2005) with respect to v.4.3.1

- Separated references to Cybertrust Qualified Certificates product

Changes in 4.3.1 (Publication Date: 10 October 2003) with respect to v.4.3

- Added SureServer product

Changes in 4.3 (Publication Date: 10 October 2003) with respect to v.4.2

- Section 1.4: Updated wording
- Section 4.3.6: Updated wording
- Section 5.13: Updated reference to logs retention period.
- Section 21.10: Updated wording
- Section 21.22: Updated wording
- Section 21.23: Updated wording

Changes in v.4.2 (Publication Date: 1 August 2003) with respect to v.4.1

- New Chapter 21 Cybertrust SureCredential 3 Qualified certificates issued under Belgian Law of 9 July 2001 implementing the European Directive 1999/93/EC of the Council and the Parliament on a Community Framework on Electronic Signatures.
- Updated Chapter 10 Cybertrust Limited Warranty Policy to include warranty requirements for product named Cybertrust SureCredential 3 Qualified certificate.
- Updated Section 5.12 on records retention period for SureCredential 3 Qualified certificate.
- Appropriate additions to the definitions list with regard to qualified certificates.



Cybertrust Certification Practice Statement

- Minor editorial updates to accommodate SureCredential 3 Qualified in the Introduction.

Acknowledgments

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

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3039: Internet X.509 Public Key Infrastructure - Qualified Certificates 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
- ETSI TS 101 862: Qualified certificate profile.
- ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).
- The ISO 1-7799 standard on security and infrastructure
- CA/Browser Forum EV Certificate Guidelines version 1.0 of June 7, 2007.

Cybertrust Certification Practice Statement

1. Introduction

This Certification Practice Statement (CPS) 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. Digital certificates can be used to create or rely upon electronic signatures. This CPS can be found on the Cybertrust CA repository at: <http://cybertrust.omniroot.com/repository.cfm>. This CPS 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 CPS 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. 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 removed from this document. 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 CPS can be found under section "Acknowledgements".

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the life cycle of certificates as 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 CPS can be addressed to:

Cybertrust
ATTN: Security Office
Ubicenter,
Philipssite 5
B-3001 Leuven,
Belgium.
Tel: + 32 (0)16 287123
Fax: + 32 (0) 16 287404
Email: corpcomp@cybertrust.com
URL: cybertrust.omniroot.com

For subscribers this CPS becomes effective and binding by accepting a subscriber agreement. For relying parties this CPS becomes binding by merely addressing a certificate related request on a Cybertrust certificate to a Cybertrust directory. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.

1.1 Overview

This CPS applies to the specific domain of the Cybertrust CA. The purpose of this CPS is to present the Cybertrust practices and procedures in managing certificates according to Cybertrust's own and

Cybertrust Certification Practice Statement

certain industry requirements pursuant to the standards set out above. This CPS applies to the above-stated domain to the exclusion of any other. This CPS aims at facilitating the Cybertrust CA in delivering certification services through discrete CAs issuing Client end entity certificates. The certificate types addressed in this CPS are the following:

SureCredential Personal	A personal certificate of medium assurance
SureCredential Professional	A personal certificate of medium assurance with reference to professional context
SureServer	A certificate to authenticate web servers
SureServer EV	A certificate to authenticate web servers *
SureServer EDU	A certificate to authenticate web servers
SureCodesign	A certificate to authenticate data objects
OmniRoot	A certificate for CAs that enter the Cybertrust hierarchy

* These certificates are issued and managed having regard to the CA/Browser Forum Guidelines for Extended Validation Certificates, which are [incorporated by reference](#) in this CPS.

Conditional upon its type, Cybertrust certificates:

- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose for them
- Can be used to authenticate web resources, such as servers and other devices.
- Can be used to digital sign code and data objects.
- Can be used to authenticate and trust other certification authorities.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of Cybertrust certificates.

A Cybertrust Certificate Policy (CP) complements this CPS. The purpose of the Cybertrust CP is, amongst others, to set out an operational rule framework for the Cybertrust CA and sub-ordinate CAs.

In addition to the CP and CPS Cybertrust maintains a range of adjacent documented policies which include but are not limited to addressing such issues as:

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

External policies, binding certificate applicants, subscribers and relying parties, are made available on line at <http://cybertrust.omniroot.com/repository.cfm>, or at such other place Cybertrust may indicate.

The exact name of the Cybertrust CA certificates that make use of this CPS are:

- GTE Cybertrust Global Root expiring in 2018
- Baltimore Cybertrust root expiring in 2025
- Cybertrust Global Root expiring in 2021

Cybertrust Certification Practice Statement

The aforementioned Cybertrust CA certificates are hereinafter, individually and collectively, referred to as the Cybertrust CA Root.

1.2 Cybertrust Certificate types

This part provides additional information on the Cybertrust certificates issued under this CPS.

1.2.1 Personal Certificates

Cybertrust offers several types of certificates for individuals, that can be used for web browsing, secure e-mail, inter organisational communications, access to personal financial information, online Internet transactions:

- **SureCredential Personal:** provides a limited identity authentication by requiring a signed copy of an identity element. These personal digital certificates for browsers are meant for low-value/low risk commercial transactions. They are valid for one, two or three years.
- **SureCredential Professional:** provides a limited identity authentication by requiring a signed copy of an identity proof. SureCredential Professional certificates require professional context affiliation. These personal digital certificates for browsers are meant for low-value/low risk commercial transactions. They are valid for one, two or three years.

1.2.2 Server Certificates

Cybertrust offers several types of certificates for servers, that can be used for web based transactions, such as the following:

- **SureServer:** SureServer is meant for entities that wish to verify their identity and participate in secured communication and transactions at the web-server level, using Secure Socket Layer (SSL) technology. The identity of the certificate-holder is authenticated by Cybertrust.
- **SureServer EV:** SureServer EV is meant for entities that wish to verify their identity and participate in secured communication and transactions at the web-server level using using Secure Socket Layer (SSL) technology. The identity of the certificate-holder is fully authenticated by Cybertrust in accordance with the CA/browser forum Guidelines for Extended Validation Certificates.
- **SureServer EDU:** SureServer EDU is meant for entities within the education and research space that wish to verify their identity and participate in secure communication and transactions at the web-server level using Secure Socket Layer (SSL) technology.

1.2.3 Object Publishing Certificates

Cybertrust offers one type of object certificate software objects:

- **SureCodeSign** provides assurance on the identity of an entity that distributes software or software object such as applets etc. on the Internet, and on the integrity of the software being distributed as well, utilizing Microsoft Authenticode or Netscape's codesigning standards.

1.2.4 Acceptable Subscriber Names

For publication in its certificates Cybertrust accepts subscriber names that are meaningful and can be authenticated as required for each product type or class.

Cybertrust Certification Practice Statement

1.2.4.1 Pseudonyms

For certain types of products Cybertrust may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law or pursuant to an otherwise legitimate request.

1.2.5 Registration procedures

For all types of certificates Cybertrust reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.

1.3 SureCredential Personal

1.3.1 General

SureCredential Personal certificates are intended for communications and transactions that require a minimum verification of the identity.

SureCredential Personal certificates are meant for communications and transactions with a low value and little risk with a need to authenticate the communicating parties and encrypt the exchange of communications.

SureCredential Personal certificates validity period is between one and three years.

SureCredential Personal certificates are issued to natural persons (individuals) only.

SureCredential Personal applicant verification is undertaken by a registration authority by using a copy of an identity proof.

SureCredential Personal certificates are issued primarily for low value and low risk personal communications and purposes.

1.3.2 Assurance Level

SureCredential Personal certificates may provide reasonable, but not foolproof, assurance of a subscriber's identity, based on an automated on-line process that compares the applicant's name, address, and other personal information on the certificate application against a signed identity proof.

Although Cybertrust's SureCredential Personal on-line identification process is a high level method of authenticating a certificate applicant's identity, it does not require the applicant's personal appearance before a registration authority.

1.3.3 Individuals:

The procedure for a certificate request can be summarized as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust such additional documentation. Upon verification of identity, Cybertrust issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate

Cybertrust Certification Practice Statement

to its device. The applicant must notify Cybertrust of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust such additional documentation. Upon verification of identity, Cybertrust issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify Cybertrust of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.3.4 Content

Information published in a SureCredential Personal certificate typically includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (Cybertrust):
- Cybertrust electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.3.5 Documents Submitted to Identify the Applicant

The applicant must submit to a Cybertrust Registration Authority a signed copy of an identification document such as an identity card, driver's licence or passport.

1.3.6 Time to Confirm Submitted Data

Cybertrust makes reasonable efforts to confirm the certificate application information and issue a digital certificate within reasonable time frames, having also regard to the verification process.

1.3.7 Issuing Procedure

The following steps describe the milestones in the procedure to issue a SureCredential Personal certificate:

- 1 The applicant chooses a strong password and submits it to an online web form along with the email address they wish to have certified by Cybertrust.
- 2 The automated system informs the applicant to check the inbox for the specified email address for further instructions.
- 3 When the applicant receives an email from the automated system, it contains a unique single use URL which the applicant is instructed to click on or load in their browser to continue.
- 4 The online web form requests the password chosen by the applicant to correlate the application in process to a validated email address that the applicant can access.
- 5 The applicant fills out the online registration form: e-mail address, common name, country code, verification method, billing information as part of the online request.
- 6 The applicant accepts online subscriber agreement.
- 7 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.).
- 8 The public key and online request are sent to Cybertrust.

Cybertrust Certification Practice Statement

- 9 Cybertrust verifies by checking copy of verification method and payment.
- 10 RA may positively verify the applicant.
- 11 Cybertrust may issue the certificate to the applicant.
- 12 Cybertrust publishes the issued certificate in on line database.
- 13 Renewal: allowed.
- 14 Revocation: allowed.

Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.

1.3.8 Limited Warranty

The warranty provided with respect to SureCredential Personal certificates is limited to the extent permitted by applicable law and further as per the applicable subscriber agreement.

1.3.9 Relevant Cybertrust Documents

The applicant must take notice and is bound by the following documents available on <http://cybertrust.omniroot.com/repository>

- 1 CPS
 - 2 Subscriber Agreement
 - 3 Data Protection Policy
- and such other documents as may be applicable and made available by Cybertrust at the aforementioned website.

1.4 SureCredential Professional

This part describes the specific requirements for SureCredential Professional certificates.

1.4.1 General

SureCredential Professional certificates are intended for certain communications and transactions that require a minimum verification of the identity.

SureCredential Professional certificates can be distributed for communications and transactions with a low value and little risk with a need to authenticate the communicating parties and encrypt the exchanged communications.

SureCredential Professional certificates validity period is between one and three years.

SureCredential Professional certificates are issued to natural persons (individuals) within their professional context only.

SureCredential Professional applicant identification is done by a registration authority by using a copy of an identity proof.

SureCredential Professional certificates are typically used primarily for intra-organisational and inter-organisational E-mail; small, "low-risk" transactions; personal/individual E-mail; password replacement; software validation; online purchases and on-line subscription services.

Cybertrust Certification Practice Statement

1.4.2 Individuals

The procedure for a certificate request can be summarized as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust such additional documentation. Upon verification of identity, Cybertrust issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to the applicant's device. The applicant must notify Cybertrust of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust such additional documentation. Upon verification of identity, Cybertrust issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify Cybertrust of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.4.3 Content

Information published in a SureCredential Professional certificate typically includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's professional organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (Cybertrust)
- Cybertrust electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.4.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit to a Cybertrust Registration Authority a signed registration form, a signed subscriber agreement and the articles of association/bylaws or proof of professional context and a copy of identity proof.

Employees are required to submit the articles of association/bylaws of their employer and obtain confirmation of their employment relationship.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a Self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

Cybertrust may require additional proof of identity in support of the verification of the applicant.

Cybertrust Certification Practice Statement

1.4.5 Time to Confirm Submitted Data

Cybertrust makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames, also having regard to the verification process.

1.4.6 Issuing Procedure

The following steps describe the milestones in the procedure to issue a SureCredential Professional certificate:

- 1 The applicant chooses a strong password and submits it to an online web form along with the email address they wish to have certified by Cybertrust.
- 2 The automated system informs the applicant to check the inbox for the specified email address for further instructions.
- 3 When the applicant receives an email from the automated system, it contains a unique single use URL which the applicant is instructed to click on or load in their browser to continue.
- 4 The online web form requests the password chosen by the applicant to correlate the application in process to a validated email address that the applicant can access. The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
- 5 The applicant accepts the on line subscriber agreement.
- 6 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.).
- 7 The public key and the online request are sent to Cybertrust automatically.
- 8 Applicant must mail to a RA copies of identity, articles of association, professional context and payment information.
- 9 RA may positively verify the applicant.
- 10 Cybertrust may issue the certificate to the applicant.
- 11 Cybertrust publishes the issued certificate in on line database.
- 12 Renewal: allowed.
- 13 Revocation: allowed.

Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.

1.4.7 Limited Warranty

The warranty provided with respect to SureCredential Professional certificates is limited to the extent permitted by applicable law and further as per the applicable subscriber agreement.

1.4.8 Relevant Cybertrust Documents

The applicant must take notice and is bound by the following documents available on <http://cybertrust.omniroot.com/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy

and such other documents as may be applicable and made available by Cybertrust at the aforementioned website.

Cybertrust Certification Practice Statement

1.5 SureServer

1.5.1 General

SureServer certificates are meant for securing communication with for example a web-site through an SSL or TLS link.

The applicant is an organisation that has an Internet Server such as a website. Server certificates are used to assure the Internet Server's identity to the visitor and to assure a confidential communication with the Internet Server.

SureServer certificates validity period is between one and three years according to the choice of the applicant.

SureServer certificates are issued to legal entities and self employed professionals registered with a professional organisation.

1.5.2 Business Entities

The procedure for a certificate request can be summarized as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link following a procedure provided by Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust the additional documentation. Upon verification of identity of the Internet Server, Cybertrust issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify Cybertrust of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust such additional documentation. Upon verification of the identity of the Internet Server, Cybertrust issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify Cybertrust of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.5.3 Content

Information published in a SureServer certificate typically includes the following elements

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (Cybertrust)
- Cybertrust electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

Cybertrust Certification Practice Statement

1.5.4 Certificate Profile

1.5.5 Documents Submitted to Identify the Applicant

The applicant must submit to a Cybertrust Registration Authority a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation.

1.5.6 Time to Confirm Submitted Data

Cybertrust makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

1.5.7 Issuing Procedure

The following steps describe the milestones in the procedure to issue a SureServer certificate as follows:

- 1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
- 2 The applicant follows the on line registration procedure.
- 3 The applicant submits the required information including organizational information, technical contact, server information, payment information.
- 4 The applicant accepts the on line subscriber agreement.
- 5 Data is sent with certificate request to Cybertrust automatically.
- 6 Cybertrust verifies the submitted information by checking organisational, payment and any other information as it sees fit. This may also include checks in third party databases or resources.
- 7 Cybertrust may positively verify the applicant.
- 8 Cybertrust may issue the certificate to the applicant.
- 9 Cybertrust publishes the issued certificate in online database
- 10 Renewal: allowed
- 11 Revocation: allowed

Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.

1.5.8 Limited Warranty

The warranty provided with respect to SureServer certificates is limited to the extent permitted by applicable law and further as per the applicable subscriber agreement.

1.5.9 Relevant Cybertrust Documents

The applicant must take notice and is bound by the following documents available on cybertrust.omniroot.com/repository:

- 1 CPS
 - 2 Subscriber Agreement
 - 3 Data Protection Policy
- and such other documents as may be applicable and made available by Cybertrust at the aforementioned website.

Cybertrust Certification Practice Statement

1.6 SureServer EV

1.6.1 General

SureServer EV certificates are used to assure the Internet Server's identity to the visitor and to assure a confidential communication with the Internet Server through an SSL or TLS link.

SureServer EV certificates validity period is between one and two years.

1.6.1.1 Extended Validation Certificates

SureServer EV certificates are issued under the minimum requirements described in the Guidelines for Extended Validation certificates. A Certificate Authority (CA) must meet such requirements in order to issue Extended Validation Certificates ("EV Certificates").

Organization information from valid EV Certificates may be displayed in a special manner by certain software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

1.6.1.2 Guidelines for Extended Validation Certificates

The Guidelines address basic issues relating to the verification of information regarding Subjects named in EV Certificates and certain related matters.

The Guidelines for Extended Validation Certificates (or EV guidelines) are an integrant part of the present Certification Practice Statement and are [incorporated by reference](#) herein.

Questions on the Guidelines for Extended Validation Certificates may be directed to the CA/Browser Forum at questions@cabforum.org.

1.6.1.3 Extended Validation Guidelines Compliance

SureServer EV certificates related sections and, if applicable, other sections of this CPS have been written out to reflect the Guidelines for EV certificates requirements.

SureServer EV issuance and management practices comply with the current version of the said Guidelines.

In the event of any inconsistencies between the SureServer EV related provisions of this document and the Guidelines for Extended Validation Certificates, the Guidelines for Extended Validation Certificates take precedence over this document.

1.6.1.4 SureServer EV Subjects

SureServer EV certificates may solely be issued to private organizations and governments entities, provided they are duly incorporated in the jurisdiction of incorporation where Cybertrust acts as a CA.

Cybertrust may not issue SureServer EV certificates to general partnerships, unincorporated associations, sole proprietorships, and individuals (natural persons).

The period retention for records fulfils professional records requirements of the Laws of the United States.

Cybertrust Certification Practice Statement

1.6.1.5 SureServer EV Issuance Specific Roles

The following applicant roles are required for the issuance of a SureServer EV Certificate

- The Certificate Requester is an applicant's employee, or an authorized agent who has express authority to represent the applicant or a third party (such as an ISP or hosting company), who is responsible for completing and submitting a Cybertrust Extended certificate request on behalf of the applicant.
- The Certificate Approver is responsible for approving the certificate request. He is an applicant's employee, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve SureServer EV Certificate Requests submitted by other Certificate Requesters.
- The Contract Signer is responsible for signing the Subscriber Agreement applicable to the requested SureServer EV Certificate. He is an applicant's employee, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

One person, whether an Applicant's employee or an authorized agent, may be authorized by the applicant to fill one, two, or all three of these roles, as the case may be.

An applicant may also authorize more than one person to fill each of these roles.

1.6.2 Business Entities

The procedure for a certificate request can be summarized as follows:

On-line: Via the Web (<https>) Prior to the issuance of a SureServer EV certificate, Cybertrust must obtain from the applicant (via a certificate Requester authorized to act on applicant's behalf) a properly signed SureServer EV certificate request that includes a certification by or on behalf of the applicant that all of the information contained therein is true and correct.

The certificate applicant submits the certificate request via a secure on-line link following a procedure provided by Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust the additional documentation. Upon verification of identity of the Internet Server, Cybertrust issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify Cybertrust of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

1.6.3 Content

Information published on a SureServer EV certificate typically includes the following elements

- Applicant's Organization Name
- Applicant's Domain Name
- Jurisdiction of Incorporation
- Registration Number (Incorporation)
- Physical Address of Place of Business (City, State, Country)
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (Cybertrust CA)
- Cybertrust electronic signature

Cybertrust Certification Practice Statement

- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.6.4 Information Submitted to Identify the Applicant

The certificate request must contain complete and accurate data relating to the following:

- Organization Name (formal legal organization name)
- Assumed Name (optional)
- Domain Name
- Jurisdiction of Incorporation (city, state, province, country)
- Incorporating Agency (name)
- Registration Number (assigned by the incorporating agency)
- Applicant Address (including phone number)
- Certificate Approver (name and contact information)
- Certificate Requester (name and contact information)

1.6.5 Data Verification

As to data verification, Cybertrust ensures that the following Subject organization information has been submitted by the applicant and shall be verified by the CA in accordance with the EV Guidelines (Sections 14 through 25) by taking all verification steps reasonably necessary:

- 1 Applicant's existence and identity, including:
 - (a) Applicant's legal existence and identity (as established with an Incorporating Agency),
 - (b) Applicant's physical existence (business presence at a physical address), and
 - (c) Applicant's operational existence (business activity)
- 2 Applicant's exclusive control of the domain name to be included in certificate;
- 3 Applicant's authorization for the SureServer EV certificate, including:
 - (a) Contract Signer, certificate Approver and certificate Requester name, title, and authority
 - (b) Subscriber Agreement signing by Contract Signer
 - (c) Approval by the certificate Approver of the certificate Request.

In this regard, Cybertrust acknowledges that a satisfactory data verification process requires an appropriate assessment of the legal and administrative practices that are applicable in the applicant's jurisdiction. Cybertrust shall consequently take all reasonable steps to conform to the said practices.

In all cases, Cybertrust is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the EV Guidelines Verification Requirement (e.g. Verification through verified Legal Opinion, verified Accountant letter, or other Qualified Independent Information Sources or Qualified Government Information source).

In addition, Cybertrust shall take reasonable steps to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks (phishing and other fraudulent schemes), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under the EV Guidelines.

Cybertrust Certification Practice Statement

1.6.5.1 Data Validation Dual Role

After all of the verification processes and procedures are completed, Cybertrust reviews all of the information and documentation assembled in support of the SureServer EV certificate and look for discrepancies or other details requiring further explanation.

Cybertrust assigns such review to a person (Validation Specialist) who is not responsible for the collection of information.

Cybertrust enforces control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of a SureServer EV certificates.

Cybertrust ensures that the Validation Specialists pass an internal examination and qualify for each skill level required by the corresponding validation task before granting privilege to perform said task

Cybertrust provides Validation Specialists with skills training that covers basic PKI knowledge, authentication and verification policies and procedures and common threats to the validation process including phishing and other social engineering tactics.

1.6.5.2 Time to Confirm Submitted Data

Cybertrust makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

1.6.5.3 Data Validity

The maximum validity period for validated data that can be used to support issuance of a SureServer EV certificate (before revalidation is required) is one year.

1.6.5.4 Issuance Prohibition

Cybertrust shall not issue any SureServer EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Place of Business is identified on any government denied list, list of prohibited persons, list of prohibited countries, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation.

1.6.6 Issuing Procedure

The issuing procedure for a SureServer EV certificate is as follows:

1. The Certificate Requester acting on behalf of the applicant follows the on line and off line registration procedure.
2. The Certificate Requester gathers the required information as specified under 1.6.4 of this CPS including but not limited to technical contact, server information, and payment information.
3. The Contract Requester ensures that the subscriber agreement is signed by the Contract Signer on behalf of the applicant.
4. The Contract Requester ensures that the certificate request is properly filled out.

Cybertrust Certification Practice Statement

5. The Certificate Requester sends both the subscriber agreement and the certificate request to Cybertrust on behalf of the applicant.
6. Cybertrust ensures that the Certificate Approver approves the certificate request submission on behalf of the applicant.
7. Cybertrust verifies the submitted information as specified under 1.6.5 of this CPS and the related provisions of the EV Guidelines incorporated by reference herein. The applicant creates a Certificate Signing Request (CSR) and a key pair using appropriate server software
8. Cybertrust may issue the certificate to the applicant.
9. Cybertrust may publish the issued certificate in an online database
10. Renewal: allowed
11. Revocation: allowed

Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.

1.6.7 Limited Warranty

1.6.7.1 Subscribers and Relying Parties

In cases where Cybertrust has issued and managed the SureServer EV certificate in compliance with these Guidelines, Cybertrust shall not be liable to the SureServer EV certificate beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such certificate beyond those specified in the CA's CPS.

In cases where Cybertrust has not issued or managed the Certificate in complete compliance with the EV Guidelines, Cybertrust may seek to limit its liability to the Subscriber and to Relying Parties for any cause of action or legal theory involved for any and all claims, losses or damages suffered as a result of the use or reliance on such SureServer EV certificate, provided that all such purported limitations must also be specified in Cybertrust CPS, and provided further that in no event shall Cybertrust seek to limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than \$2,000 per Subscriber or Relying Party per SureServer EV certificate.

1.6.7.2 Indemnification of Application Software Vendors

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, Cybertrust acknowledges that the Application Software Vendors who has a root certificate distribution agreement in place do not assume any obligation or potential liability of Cybertrust under these Guidelines or that otherwise might exist because of the issuance or maintenance of SureServer EV certificates or reliance thereon by Relying Parties or others.

Thus, Cybertrust shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to a SureServer EV Certificate, regardless of the cause of action or legal theory involved.

This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to a SureServer EV certificate issued by Cybertrust where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy a SureServer EV certificate this is still valid, or displaying as trustworthy: (1) a SureServer EV certificate that has expired, or (2) a SureServer EV certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the browser software either failed to check such status or ignored an indication of revoked status).

Cybertrust Certification Practice Statement

1.6.7.3 Root CA Indemnification

In cases where the Subordinate CA and the Root CA are different legal entities and the Root CA specifically enables the Subordinate CA to issue SureServer EV Subscriber Certificates, the Root CA shall also be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with the EV Guidelines, and for all liabilities and indemnification obligations of the Subordinate CA under the EV Guidelines, as if the Root CA was the Subordinate CA issuing the SureServer EV Certificates.

However, this Section shall not apply to cases where a Root CA, Root CA "A", from a different legal entity, cross-certifies Root CA "B" to enable certificates issued by "B" to be trusted in older, non-EV enabled browsers. The cross certificate issued by "A" to "B" does not enable EV according to these guidelines. Certificates issued by "B" are EV enabled only when an EV enabled browser can build a certificate chain to the root certificate of "B".

1.6.8 Insurance Plan

As to SureServer EV Certificates, Cybertrust maintains an appropriate insurance related to its respective performance and obligations under this CPS and the EV Guidelines.

1.6.9 Relevant Cybertrust Documents

The applicant must take notice and is bound by the following documents available on cybertrust.omniroot.com/repository:

- 1 Cybertrust CPS
- 2 Subscriber Agreement
- 3 CA/Browser Forum Guidelines for Extended Validation Certificates

1.7 SureServer EDU

1.7.1 General

SureServer EDU certificates are meant for secured communication with for example a web-site through an SSL or TLS link.

The applicant is an organisation within the educational or research environment that has an Internet Server such as a website. Server certificates are used to assure the Internet Server's identity to the visitor and to assure a confidential communication with the Internet Server.

SureServer EDU certificates validity period is between one and three years.

SureServer EDU certificates are issued to entities and self employed professionals registered with a professional organisation which is operating in the educational or research space.

The period retention for records fulfils professional records requirements of the Laws of the Belgium.

1.7.2 Business Entities

The procedure for a certificate request can be summarized as follows:

On-line: Via the Web (<https>). The certificate applicant submits an application via a secure on-line link following a procedure provided by Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to

Cybertrust Certification Practice Statement

Cybertrust the additional documentation. Upon verification of identity of the Internet Server, Cybertrust issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify Cybertrust of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

1.7.3 Content

information published in a SureServer EDU certificate typically includes the following elements

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (Cybertrust CA or Cybertrust CA)
- Cybertrust electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.7.4 Information Submitted to Identify the Applicant

The applicant must provide business and contact details to Cybertrust and underwrite those by click-through process. Cybertrust has the right to request a signed registration form, a signed subscriber agreement, the articles of association of the applying organisation and proof of the applying organisation belonging to the educational or research market if it deems necessary. Independent verification through consulting industry or other database with telephone confirmation will be performed.

1.7.5 Time to Confirm Submitted Data

Cybertrust makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

1.7.6 Issuing Procedure

The following steps describe the milestones in the procedure to issue a SureCredential Professional certificate:

- 1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
- 2 The applicant follows the on line registration procedure.
- 3 The applicant submits the required information including organizational information, technical contact, server information and if required payment information.
- 4 The applicant accepts by click-through the on line subscriber agreement.
- 5 Data is sent with certificate request to Cybertrust automatically.
- 6 Cybertrust verifies the submitted information by checking organisational and any other information as it sees fit. This may also include checks in third party databases or resources and independent verification through telephone.
- 7 Cybertrust may positively verify the applicant.
- 8 Cybertrust may issue the certificate to the applicant.
- 9 Cybertrust publishes the issued certificate in online database
- 10 Renewal: allowed

Cybertrust Certification Practice Statement

11 Revocation: allowed

Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.

1.7.7 Limited Warranty

To the extent permitted by applicable law, SureServer EDU certificates are provided “as is” without any warranty. Cybertrust accepts no liability and offers no insurance with respect to SureServer EDU certificates.

1.7.8 Relevant Cybertrust Documents

The applicant must take notice and is bound by the following documents available on <http://cybertrust.omniroot.com/repository>

- 1 Cybertrust CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy

and such other documents as may be applicable and made available by Cybertrust at the aforementioned website.

1.8 SureCodesign

1.8.1 General

SureCodesign certificates are used for the signing of software objects, such as software packages or applets.

SureCodesign certificates validity period is between one and three years.

SureCodesign certificates are issued to legal entities and self-employed professionals.

1.8.2 Business Entities

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust such additional documentation. Upon verification of identity, Cybertrust issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify Cybertrust of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to Cybertrust. Additional documentation in support of the application may be required so that Cybertrust verifies the identity of the applicant. The applicant submits to Cybertrust the additional documentation. Upon verification of identity, Cybertrust issues the certificate and sends the certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify

Cybertrust Certification Practice Statement

Cybertrust of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.8.3 Content

Information published on a SureCodesign certificate typically includes the following elements:

- Applicant's e-mail address
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (Cybertrust)
- Cybertrust electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.8.4 Documents Submitted to Identify the Applicant

The applicant must submit to a Cybertrust Registration Authority a copy of identity proof such as an identity card, driver's license or passport and the articles of association of the applying organisation (if applicable).

1.8.5 Time to Confirm Submitted Data

Cybertrust makes reasonable efforts to confirm certificate application information and issue a digital certificate within the reasonable time frames.

1.8.6 Issuing Procedure

The procedure for a certificate request can be summarized as follows:

:

- 1 The applicant fills out online the registration form: e-mail address, organizational info, common name, country code, payment info
- 2 The applicant accepts the online subscriber agreement
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
- 4 The public key and online request are sent to Cybertrust automatically
- 5 Cybertrust verifies the submitted information by checking organisational, payment and any other information as it sees fit also through third party databases or resources. This may also include checks in third party databases or resources and independent verification through telephone.
- 6 Cybertrust may positively verify the applicant.
- 7 Cybertrust may issue the certificate to the applicant.
- 8 Cybertrust publishes the issued certificate in an online database
- 9 Renewal: allowed
- 10 Revocation: allowed

Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.

1.8.7 Limited Warranty

The warranty provided with respect to SureCodesign certificates is limited to the extent permitted by applicable law and further as per the applicable subscriber agreement..

Cybertrust Certification Practice Statement

1.8.8 Relevant Cybertrust Legal Documents

The applicant must take notice and is bound by the following documents available on <http://cybertrust.omniroot.com/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy

and such other documents as may be applicable and made available by Cybertrust at the aforementioned website.

1.9 Certificate usages

Certain limitations apply to the use of Cybertrust certificates. A Cybertrust certificate can only be used for purposes explicitly permitted as they are listed below:

Electronic signature: Electronic signature can only be used for specific electronic transactions that support electronic signing of electronic forms, electronic documents, electronic mail etc. The signature certificate is only warranted to produce electronic signatures in the context of applications that support digital certificates. To describe the function of an electronic signature, the term non-repudiation is often used. Certificates that are appropriate for electronic signature are the following:

SureCredential Personal: non repudiation of a transaction (medium level)

SureCredential Professional: non repudiation of the transaction by a party acting in an organisational context (medium level)

Authentication (Users): User authentication certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a digital certificate. To describe the function of authentication, the term digital signature is often used.

- **SureCredential Personal:** authentication of a natural person (medium level)
- **SureCredential Professional:** authentication of a natural person within an organisational context (medium level)

Authentication (Devices and objects): Device authentication certificates can be used for specific electronic authentication transactions that support the identifying of web sites and other on line resources, such as software objects etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used.

- **SureServer:** authentication of a remote domain name and webservice and encryption of the communication channel.
- **SureServer EV:** authentication of a remote domain name and webservice and encryption of the communication channel.
- **SureServer EDU:** authentication of a remote domain name and webservice and encryption of the communication channel.
- **SureCodesign:** authentication of a data object.

Confidentiality: All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality is required to assure the confidentiality of

Cybertrust Certification Practice Statement

business and personal communications as well as for purposes of personal data protection and privacy.

Any other use of a digital certificate is not supported by this CPS. When using a digital certificate the functions of electronic signature (non repudiation) and authentication (digital signature) are permitted together with the same certificate.

1.10 Document Name and Identification

Cybertrust ensures compliance of its certificates with the requirements and assertions of this CPS.

1.11 PKI participants

The Cybertrust CA makes its services available to Cybertrust subscribers. These subscribers may, by way of an example, include natural persons and legal entities that use certificates for the purposes of:

- Authentication (digital signature); and/or
- Electronic signature (non-repudiation); and/or
- Encryption

under the terms and conditions of the applicable subscriber agreement.

1.11.1 Cybertrust Certification Authority

A Certification Authority, such as Cybertrust, is an organisation that issues digital certificates to be used in public or private domains, within a business framework, a transactions context etc. A certification authority is also referred to as the Issuing Authority to denote the purpose of issuing certificates at the request of an RA.

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 provides the services pertaining to the management of certificates under the Cybertrust CA Root. The Cybertrust CA also manages a core online registration system for all certificate types, issued under the Cybertrust CA Root.

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 on directories of issued certificates. The Cybertrust CA operates such directories.

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

- Issuance
- Revocation
- Re-Key
- Status validation
- Directory service

Cybertrust Certification Practice Statement

Some of the tasks attributed to the certificate lifecycle are delegated to selected Cybertrust RAs that operate on the basis of a service agreement with Cybertrust.

1.11.1.1 Roles of Cybertrust

Cybertrust operates under two discreet roles.

Firstly, 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.

Secondly Cybertrust operates an international network of Trusted Third Parties (TTP's) sharing the Cybertrust procedures and using suitable brand name to issue trusted digital certificates to public and private entities. Such partners include Cybertrust accredited Certification Authorities and RAs that operate under an agreement with Cybertrust. This role may be limited to the issuance of certificates to other certification authorities, which seek to inherit trust that is usually vested in the Cybertrust CA root and brand name.

1.11.1.2 Cybertrust root and hierarchy

Cybertrust makes available to subscribers a dedicated root hierarchy to ensure the integrity of the end user certificate and the uniqueness of the resources made available for digital certificates. The Cybertrust CA manages a broader range of the Cybertrust trust network that includes roots that have been set up to fulfil specific purposes such as the issuance of end user certificates at levels defined by Cybertrust etc. as well as other participating CAs that benefit from Cybertrust's root, which is embedded in applications. The Cybertrust Certificate Policy addresses the Root level of the Cybertrust hierarchy.

The roots that are addressed under this CPS include roots used for issuing the following type of certificates:

- SureCredential Personal
- SureCredential Professional
- SureServer
- SureServer EV
- SureServer EDU
- SureCodesign

1.11.2 Cybertrust Registration Authorities

The Cybertrust CA reaches its subscribers through designated Registration Authorities ('RA'). An RA requests the issuance, suspension and revocation of a certificate under this CPS. An RA submits the necessary data for the generation and revocation of the certificates to the CA.

1.11.2.1 RA role description

A Cybertrust RA interacts with the subscriber to perform its role in the provision of public certificate management services. A Cybertrust RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to Cybertrust CA certification services.

Cybertrust Certification Practice Statement

- 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, notify the Cybertrust CA to issue a certificate.
- Initiates the process to suspend, or unsuspend or revoke a certificate and request a certificate revocation from the Cybertrust CA Root.

The Cybertrust RA acts pursuant to an agreement with Cybertrust under which it must act in accordance with the approved practices and procedures of the Cybertrust CA including this CPS and documented Cybertrust RA procedures.

In order to issue certain specific types of certificates, Cybertrust RAs might need to rely on certificates issued by third party certification authorities or other third party databases and sources of information. Identity cards and drivers licenses are such sources of authoritative subscriber information. Relying Parties are hereby prompted to seek specific information by referring to the appropriate certificate policies prevailing in managing specific certificate types issued under the Cybertrust Root.

If successful, the evaluation is followed by the issuance of the certificate to the applicant organisation.

Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of RAs.

1.11.2.2 RA specific requirements for SureServer EV certificates

For the issuance of SureServer EV certificates, Cybertrust contractually obligates each RA and/or subcontractor to comply with all applicable requirements in the [EV Guidelines](#) incorporated by reference herein and to perform them as required of the CA itself.

Under the terms of the EV Guidelines, Cybertrust may contractually authorize the Subject of a specified valid EV certificate to perform the RA function and authorize Cybertrust to issue additional EV Certificates at third and higher domain levels that contain the domain that was included in the original EV Certificate (also known as "Enterprise EV Certificates"). In such case, the Subject shall be considered an Enterprise RA, and shall not authorize the CA to issue any SureServer EV certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA.

Cybertrust shall not delegate the performance of the Final Cross-Correlation and Due Diligence requirements of Section 24 of Extended Validation Guidelines, which are briefly described under this CPS (1.6.1.5 - final paragraph).

1.11.3 Subscribers

Subscribers of Cybertrust services are natural or legal persons that successfully apply for a certificate. Subscribers use electronic signature services within the domain of the Cybertrust. 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.

Cybertrust Certification Practice Statement

Natural persons that are subscribers typically hold a valid identification document, such as an identity card, passport or equivalent, which is used as credential in order to issue electronic certificates.

Legal persons are identified on the basis of the published by-laws and appointment of Director as well as the subsequent government gazette or other third party databases. Self-employed are identified on the basis of proof of professional registration supplied by the competent authority in the country in which they reside.

For all categories of subscribers, additional credentials are required as explained on the online process for the application for a certificate.

Subscribers of end entity certificates issued under the Cybertrust CA include employees and agents involved in day-to-day activities within Cybertrust that require accessing Cybertrust network resources.

Subscribers are also sometimes operational or legal owners of signature creation devices that are issued with for the purpose of generating a key pair and storing a certificate.

It is expected that a subscriber organisation has an employment or service agreement or otherwise a pre-existing contract relationship with Cybertrust authorising it to carry out a specific function within the scope of an application that uses Cybertrust certificate services. Granting a certificate to a subscriber organisation is only permitted pursuant to such an agreement between Cybertrust and the subscribing end entity.

1.11.4 Subjects

Subjects of Cybertrust CA certificates services are persons or entities that are subscribers or are associated with a subscriber. 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.

Natural persons can be listed as subjects of the following certificates:

- SureCredential Personal
- SureCredential Professional

Legal entities created through all recognized forms of incorporation or government entities can be listed as subjects of the following certificates:

- SureServer EV

Legal persons or self-employed professionals can be listed as subjects of the following certificates:

- SureServer
- SureServer EDU
- SureCodeSign

Cybertrust Certification Practice Statement

1.11.5 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 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.

1.11.6 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 Cybertrust CA revocation information, currently a Certificate Revocation List (CRL). Certificate 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 CPS.

1.12 Certificate use

Certain limitations apply to the use of Cybertrust CA certificates.

1.12.1 Appropriate certificate usage

Certificates issued under the Cybertrust CA can be used for public domain transactions that require:

- Non-repudiation and
- Authentication
- Confidentiality

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

1.12.2 Prohibited certificate usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorised. Cybertrust certificates are not authorised for use within Closed Groups unless such Groups have notified Cybertrust thereof and Cybertrust has consented to it.

1.12.3 Certificate extensions

Cybertrust issues certificates that contain extensions defined by the X.509 v.3 standard other standards as well as any other formats including those used by Microsoft and Netscape.

Cybertrust Certification Practice Statement

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.

As 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, and other data.

A certificate policy extension limits the usage of a certificate to the requirements of a business or a legal context.

1.12.4 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.

1.13 Policy Administration

The Cybertrust CA is a top 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 Cybertrust CPS. The Cybertrust CA registers, observes the maintenance, and interprets this CPS. The Cybertrust CA makes available the operational conditions prevailing in the life-cycle management of certificates issued under the Cybertrust CA root.

1.13.1 Scope

In an effort to invoke credibility and Trust in the Cybertrust CPS 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 issued on or after the date of the publication of the updated version of the CP and/or CPS.

1.13.2 Cybertrust Policy Management Authority

New versions and publicized updates of Cybertrust policies are approved by the Cybertrust Policy Management Authority. The 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 Cybertrust Policy Management Authority ex officio.

All members of the 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 Cybertrust Policy Management Authority counts double.

Cybertrust Certification Practice Statement

1.13.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the Cybertrust Policy Management Authority that CPS is published in the Cybertrust online Repository at <http://cybertrust.omniroot.com/repository>.

Cybertrust publishes a notice of such updates on its public web site, currently located at <http://cybertrust.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 CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the Cybertrust CPS.

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 current and immediately preceding versions of its CPS.

1.13.3.1 Changes with notification

Updated versions of this CPS are notified to parties that have a legal duty to receive such updates, e.g. auditors with a specific mandate to do so.

1.13.4 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. 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

1.14 Definitions and acronyms

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

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 on 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 CPS. 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, internal security policies etc. However these elements are disclosed in audits associated with formal accreditation schemes that Cybertrust may subject itself to, such as Web Trust for CAs and EV WebTrust for CA.

2.1 Access control on repositories

While Cybertrust strives to keep access to its public repository and access to its policy is (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 operates RAs that verify and authenticate the identity and/or other attributes of an end-user certificate applicant for a certificate.

Prior to requesting the CA to issue a certificate, Cybertrust RAs verify the identity of applicants of a certificate.

Cybertrust RAs maintain appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

Cybertrust RAs authenticate the requests of parties wishing to revoke certificates under this policy.

3.1 Naming

To identify a subscriber, the Cybertrust CA follows and the Cybertrust RAs apply certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names, RFC-822 names or X.400 names. The Cybertrust CA issues certificates to applicants that submit a documented application containing a verifiable name.

3.2 Initial Identity Validation

The identification of the applicant for a certificate is carried out according to a documented procedure to be implemented by the Cybertrust RAs.

For the identification and authentication procedures of the initial subscriber registration Cybertrust takes the following steps:

- The natural person identified in the subject field must demonstrate possession of the private key corresponding to the public key presented to the Cybertrust CA. The subject itself or its designated representative must demonstrate this.
- Cybertrust RAs might rely on such resources as third party databases to identify and authenticate natural persons applying for a certificate.

For the identification and authentication of appropriately authorised third party agents applying for a Cybertrust certificate controls include the following:

- Controlling physical identification documents such as an identity card or passport issued by a designated authority in the country of origin of the applicant.
- Authenticating the identity of the applicant based on other documentation or credentials provided.
- Requesting an applicant to physically appear before a Cybertrust RA prior to issuing a certificate.
- Requesting a third party agent or his/her principal (e.g. a Cybertrust contractor) to produce evidence with regard to the relationship between Cybertrust and the third party agent (e.g. an outsource contract etc.).

Cybertrust Certification Practice Statement

A Cybertrust RA may refuse issuing a certificate to an applicant unless sufficient evidenced is produced with regard to the applicant's identity. If an application is rejected applicants may subsequently reapply.

To issue certificates, a Cybertrust RA endeavours to provide the applicant with sufficient credentials (enrolment URL, password) such that the enrolment process can then proceed online.

At Cybertrust's discretion any such credentials may be two-factor, communicated by independent channels using agreed and proven contact methods.

The identification of an applicant for a certificate is carried out according to a documented procedure to be implemented by the Cybertrust RAs.

3.3 Subscriber registration process

Unless otherwise provided in this CPS in connection with the EV guidelines (SureServer EV certificates), the following rules applies as to the Subscriber Registration Process.

Cybertrust ensures that:

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

In particular:

- Cybertrust provides notice to the applicant through its web site at www.cybertrust.com and the dedicated policy framework published on its repository at cybertrust.omniroot.com/repository.
- Before entering any contractual relationship with the subscriber, Cybertrust makes available a subscriber agreement, which the applicant must approve prior to placing a request with Cybertrust. This agreement can also be consulted in advance on Cybertrust's repository at cybertrust.omniroot.com/repository.
- Cybertrust's policy framework is limited under data protection and consumer protection laws and applicable warranty limitations, as explained in the Cybertrust CPS.
- 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 typically verifies by appropriate means and on the basis of a documented procedure, the identity and, if applicable, all specific attributes thereof of applicants of certificates.

Evidence on identity is checked against a natural person either directly or indirectly using means which provide equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation. Examples of evidence checked indirectly against a natural person is documentation presented for registration that was acquired as the result of an application requiring physical presence.

Evidence on identity of organizations is checked against documents presented to establish the existence of organizations or through independent verification through third-party databases. Submitted evidence may be in the form of either paper or electronic documentation.

Cybertrust Certification Practice Statement

Self-employed professionals that are eligible to be issued with certificates typically have to prove their identity as individuals as well as their professional registration.

Specific documents required include the following:

3.3.1.1 SureCredential Personal

The applicant must submit to a Cybertrust Registration Authority a signed copy of an identification document such as an identity card, driver's licence or passport.

3.3.1.2 SureCredential Professional

In all cases, the applicant must submit to a Cybertrust Registration Authority a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

Employees are required to submit the articles of association of their employer and obtain confirmation of their employment relationship.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

Cybertrust may require additional proof of identity in support of the verification of the applicant.

3.3.1.3 SureServer

The applicant must submit to a Cybertrust Registration Authority a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation. Cybertrust may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.1.4 SureServer EV

The applicant (the Certificate Requester) must submit to a Cybertrust Registration Authority a registration form and a subscriber agreement, approved by the Certificate Approver and signed by the Certificate Signer to in accordance with the EV guidelines which are incorporated by reference herein. .

Cybertrust may require additional identification proof in support of the verification of the applicant's identity according to the EV Guidelines.

3.3.1.5 SureServer EDU

The applicant must submit to Cybertrust Registration Authority a registration form and a Subscriber Agreement, both accepted and agreed to through a click-through acceptance process.

Cybertrust Certification Practice Statement

Cybertrust may require additional identification proof in support of the verification of the applicant's identity.

3.3.1.6 SureCodesign

The applicant must submit to a Cybertrust Registration Authority a copy of identity proof such as an identity card, driver's license or passport and the articles of association of the applying organisation (if applicable).

Cybertrust may require additional identification proof in support of the verification of the applicant's identity.

3.3.2 Data needed for subscriber registration

Where an applicant is natural person evidence shall be provided of the following data prior to accepting an application for a certificate:

- Full name (including surname and given names).
- Date of birth
- Place of birth
- A nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

Where the subscriber is a person who is identified in association with an organizational entity, proof will be produced in terms of:

- 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.

Where the subscriber is an organization, proof will be produced in terms of:

- Full name and legal status of the associated legal person of the organizational entity.
- Company registration number, VAT number or other attributes of the subscriber which may be used to, as far as possible, distinguish it from others with a similar same name.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that any natural person involved in the application process is associated with that organizational entity.

Cybertrust neither recommends nor encourages any specific choice of an end user product. Applicants and subscribers are entirely responsible to make the appropriate requests for the issuance of their certificates.

3.3.3 Pseudonyms

Cybertrust may conditionally accept the use of pseudonyms in its certificates. Cybertrust reserves its right to refuse granting a pseudonym certificate following a reasonably justified application assessment. Reasons for rejecting a pseudonym application include but are not limited to a pseudonym being:

Cybertrust Certification Practice Statement

- Already is use
- Violating third party rights
- Constituting slander etc.

Cybertrust maintains documented records of a pseudonym application and application rejections.

Notice is hereby given that Cybertrust may disclose the real identity of the pseudonym certificate holder to any party, which can demonstrate a justified and legitimate interest to it.

The subscriber provides a physical address, or other attributes, which describe how the subscriber may be contacted.

Cybertrust reserves its right to insert names with pseudonyms in its certificates on a case-by-case basis. Cybertrust might make such designations in guidance documentation supplied to its RAs

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 subscriber agreement and any material or documents that support the application which also include but are not limited to:

- Cybertrust subscriber 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 CPS in the case of the CA terminating its services.
- That information held in the certificate is correct and accurate.
- Full name 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.
- A specifically designed attribute that uniquely identifies the applicant within the context of the Cybertrust CA.
- Proof of organization context where necessary.
- 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.
- Any evidence produced in support of an application with a pseudonym.

A Cybertrust RA maintains such records. For organizational purposes a Cybertrust RA may also maintain duplicates of these records for a shorter period of time.

3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests of its subject types (CA, RA, subscriber, and other participants) Cybertrust requires using an online authentication mechanism (e.g. digital certificate authentication, PIN etc.) and a request addressed to the Cybertrust CA or an RA.

4. Certificate Life-Cycle Operational Requirements

Unless otherwise provided in this CPS in connection with the EV guidelines (SureServer EV certificates), the following operational requirements apply to Certificate Life-Cycle.

All entities within the Cybertrust domain including the 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 gets revoked.

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

To carry out its tasks Cybertrust may use third party agents. Cybertrust assumes full responsibility and accountability for all acts or omissions of all third party agents it may use to deliver services associated with CA operations within the Cybertrust CA.

4.1 Certificate Application

A Cybertrust RA has the duty to provide the Cybertrust CA with accurate information on certificate requests it lodges on behalf of the end user applicants.

The Cybertrust CA acts upon request of an RA that has the authority to make a request to issue a certificate.

Subscribers undergo an enrolment process that requires:

- a. Filling out an application form.
- b. Generating a key pair, directly or through an agent.
- c. Delivering the generated public key corresponding to a private key to Cybertrust CA.
- d. Accepting the subscriber agreement.

In case of a subject that can be distinguished from a subscriber, then the above listed requirements (a) through to (d), are met by the subject; else, the subject's designated applicant meets them. The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the Cybertrust CA. The subscriber agreement incorporates by reference this CPS.

In general, an online enrolment process will be sufficient, only as explicitly permitted by Cybertrust.

In all other cases (including EV certificates) credentials are requested, as appropriate, in a way that the exact identity of the applicant can reasonably be established. This includes a manually signed copy of the subscriber agreement, and a copy of identity card, or physical appearance before the RA.

4.2 Certificate Application Processing

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.

Cybertrust Certification Practice Statement

The RA acts upon a certificate application to validate an applicant's identity as foreseen in a documented procedure.

Pursuant to a certificate application the RA either approves or rejects a certificate application. If the application is approved the RA transmits the registration data to Cybertrust.

For rejected applications of certificate requests, the RA notes the reason for rejecting the application.

4.3 Certificate Issuance

The Cybertrust RA subsequently 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.

The Cybertrust CA verifies the identity of the Cybertrust RA on the basis of credentials presented (a special RA administrator certificate). The Cybertrust CA retains its right to reject the application, or any applicant for RA certificates.

Following issuance of the certificate, the Cybertrust CA delivers the issued certificate to the subscriber directly or through an agent.

4.4 Certificate generation

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

- The procedure to issue a certificate is securely linked to the associated registration, including the provision of any subscriber generated public key.
- The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket layer) links, especially when the applicant carries out CA/RA communications.
- The authentication of registrars is ensured through appropriate credentials issued to them.
- Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.
- Cybertrust verifies that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are ever used.
- 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.

Any objection to accepting an issued certificate must explicitly be notified to the Cybertrust CA. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

Cybertrust Certification Practice Statement

The Cybertrust CA might post the issued certificate on a repository (X.500 or LDAP). The Cybertrust CA also reserves its right to notify the certificate issuance by the Cybertrust CA to other entities.

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

Unless otherwise stated in this CPS, the duties of subscribers include the following:

1. Accepting all applicable terms and conditions in the CPS 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.
7. For any acts and omissions of partners and agents subscribers use 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. Request the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a Cybertrust CA certificate.
10. Refraining from tampering with a certificate.
11. Only using certificates for legal and authorised purposes in accordance with the CPS.
12. Refrain from using a certificate outside possible license restrictions imposed by Cybertrust.

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.

4.6.1.1.1 Certificate Life-Cycle Operational Requirements

Subscribers are hereby notified of their 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 or through an agent.

Cybertrust issues, revokes or suspends certificates only at the request of the RA following a successful application of a certificate applicant.

Cybertrust Certification Practice Statement

4.6.1.2 Subscriber Duty Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CP, subscribers have a duty to refrain from any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

4.6.1.3 Reliance 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 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 CA Repositories and web site may result in terminating the relationship between the Cybertrust CA and the party.

4.6.2 Relying party

The duties of a relying party are as follows:

4.6.2.1 Relying party duties

A party relying on a Cybertrust 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 CA 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 suspended or revoked.
- Validate at least those certificate attributes that materially affect the relying party's own signature policy or practices.

4.6.2.2 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 CPS and any other conditions of use that the Cybertrust CA may make available. Parties demonstrate acceptance of the conditions of usage of the CPS 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:

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

4.7 Certificate Renewal

Subscribers may request the renewal of Cybertrust certificates. To request the renewal of a Cybertrust certificate, an end user lodges an online request. The renewal of a Cybertrust certificate consists in essence of re-keying : a new public key is digitally signed.

Requirements for renewal of certificates, where available, may vary from those originally required for subscribing to the service.

Before renewing a SureServer EV certificate, Cybertrust must perform all authentication and verification tasks required by the EV Guidelines to ensure that the renewal request is properly authorized by the Applicant and that the information displayed in the SureServer EV certificate is still accurate and valid.

4.8 Certificate Revocation and Suspension

Cybertrust shall use reasonable efforts to publish clear guidelines for revoking certificates, and maintain a 24/7 ability to accept and respond to revocation requests.

The identification of the subscriber who applies for a revocation of a certificate is carried out according to an internal documented procedure. This procedure is subject to auditing by authorised parties in compliance with the requirements set by the accreditation schemes Cybertrust subjects to.

Subject to prior agreement with Cybertrust any Cybertrust RA may carry out the identification and authentication of holders seeking to revoke a certificate. To this effect an authenticated request is needed to initiate the procedure. The requesting party will have to be authenticated as the subscriber of that certificate or at least as an authorised agent of the subscriber of the certificate.

An RA might further challenge the requesting party until its identity is sufficiently established and distinguished from others.

Revocation and suspension requests can also be placed directly to the Cybertrust RA at the following correspondence address:

Cybertrust, Philipssite 5, B-3001, Leuven, Belgium or midsupport@Cybertrust.com.

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

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject.
- The certificate's subject or their appointed subscriber has breached a material obligation under this CPS.
- The performance of a person's obligations under this CPS 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. 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 Certification Practice Statement

Cybertrust does not provide suspension services 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.

For SureServer EV certificates, revocation shall be mandatory when the Cybertrust CA determines, in its sole discretion that the certificate was not issued in accordance with the terms and conditions of the EV guidelines.

4.8.1 Term and Termination of Suspension and Revocation

Suspension may last for a maximum of seven calendar days to establish the conditions that caused the request of suspension.

The Cybertrust CA publishes notices of suspended or revoked certificates in the Cybertrust CA repository. The Cybertrust CA may publish its suspended or revoked certificates in its CRL and additionally, by any other means as it sees fit.

4.9 Certificate Status Services

The Cybertrust CA makes available certificate status checking services including CRLs, , and appropriate Web interfaces.

CRL

A CRL lists all revoked and suspended certificates during the application period. CRLs for the different products are available from <http://crl.omniroot.com/>

A CRL is typically issued every 3 hours.

4.10 End of Subscription

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

4.11 Certificates Problem Reporting and Response Capability

In addition to certificate revocation, Cybertrust provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to certificates. Cybertrust shall use reasonable efforts to provide a 24x7 capability to accept and acknowledge and respond to such reports.

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.

Unless otherwise provided in this CPS in connection with the EV guidelines (SureServer EV certificates), the following requirements apply to management, operational, and physical controls:

5.1 Physical Security Controls

The Cybertrust CA implements physical controls on its own, leased or rented premises.

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

Physical access is restricted by implementing 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 a token 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 obtains a signed statement from each member of staff for maintaining confidentiality and protecting personal data.

All members of the staff operating the 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 Certification Practice Statement

The Cybertrust CA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted members of the Cybertrust CA staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The Cybertrust CA ensures that all actions with respect to the Cybertrust CA can be attributed to the system and the person of the CA that has performed the action.

The Cybertrust CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The Cybertrust CA performs checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks are specifically directed towards. Background checks may include:

- Search of criminal record
- Check of professional references
- Confirmation of previous employment
- Confirmation of the most relevant educational degree obtained
- Check of representations made by the candidate.
- Any other as it might be deemed necessary.

5.3.2 Background Checks and Clearance Procedures

The Cybertrust CA makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or self-declarations.

5.3.3 Training Requirements and Procedures

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

5.3.4 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.

5.3.5 Job Rotation

Not applicable.

5.3.6 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.

Cybertrust Certification Practice Statement

5.3.7 Controls of independent contractors

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

5.3.8 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 that include but are not limited to

- Issuance of a certificate
- Revocation of a certificate
- Suspension of a certificate
- Publishing of a CRL

Audit trail records contain:

- The identification of the operation
- The data 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 reviews log files at regular intervals and detects and reports 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 should be properly protected by an access control mechanism. Log files and audit trails are backed up and must be available to independent auditors upon request.

Auditing events are not given log notice.

5.5 Records Archival

Cybertrust CA keeps archives in a retrievable format.

Cybertrust Certification Practice Statement

Cybertrust CA ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of Cybertrust CA and the RA as appropriate.

The Cybertrust CA keeps internal records of the following items:

- All certificates for a period of a minimum of 1 year after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 1 year after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 1 year following the revocation of a certificate.
- CRLs for a minimum of 1 year after expiration or revocation of a certificate.
- Support documents on the issuance of certificates for a period of 5 years after expiration of a certificate.

Cybertrust maintains records for a period of 5 years for the following products:

- SureCredential Professional
- SureServer
- SureCodesign

Cybertrust maintains records for a period of 7 years for the following products:

- SureServer EV

As regards to such products, Cybertrust records in detail every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records must be available as auditable proof of the CA's practices. The foregoing also applies to all registration agents (RAs) and subcontractors as well.

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 certificates for at least 1 year.

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:

- 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 Archive Collection

The Cybertrust CA archive collection system is internal.

Cybertrust Certification Practice Statement

5.5.5 Procedures to obtain and verify archive information

To obtain and verify archive information Cybertrust CA maintains records under clear hierarchical control.

The 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 or in paper-based format or any other format that the Cybertrust CA may see fit.

The Cybertrust CA may revise record retention terms as it might be required in order to comply with accreditation schemes including WebTrust for CAs, and the CA/browser forum EV Guidelines.

5.6 Compromise and Disaster Recovery

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

The Cybertrust CA establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

A business continuity plan has been implemented to ensure business continuity following a natural or other disaster.

In case of suspected or known compromise of Cybertrust CA private key, Cybertrust Crisis Management procedures are enacted according to the Incident Management process. and with approval from Cybertrust senior management. Notification to involved parties is performed through the communication plan and in CASE of CA Certificate revocation is required, the revoked status is communicated to relying parties through Cybertrust CRL Website at URL : <http://crl.omniroot.com/>.

Cybertrust has developed the capability to recover its CA operations within twelve (12) business hours following a disaster with support for all the key functions i.e. certificate issuance, certificate revocation, and publication of CRL information.

As to the products issued under the EV guidelines, Cybertrust undertakes to develop, implement, and maintain a comprehensive Security Program reasonably designed to protect the confidentiality, integrity, and availability of the EV Data and EV Processes and comply with other security requirements applicable to the CA by law.

Cybertrust comprehensive Security Program includes a security plan base on a risk assessments document whereby the CA develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the EV Data and EV Processes, as well as the complexity and scope of the activities of the CA. Such Security Plan shall include administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the CA's business and the EV Data and EV Processes. Such Security Plan shall also take into account then-available technology and the cost of implementing the specific measures, and must implement a reasonable

Cybertrust Certification Practice Statement

level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected. 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 the Cybertrust CA.

6. Technical Security Controls

This section sets out the security measures taken by the 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

The Cybertrust CA protects its private key(s) in accordance with this CPS. The Cybertrust CA uses private signing keys only for signing CRLs, and OCSP responses in accordance with the intended use of each of these keys.

The Cybertrust CA will refrain from using its private keys used within the 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 secret shares of its private key(s).

6.1.1.1 Cybertrust 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.

6.1.1.2 Cybertrust CA Private Key Type

For the CA Root key it uses, the Cybertrust CA makes use of the RSA algorithm with a key length of 1024 or 2048 bits and a validity period of at least 14 years.

For the operational CA keys it uses the Cybertrust CA makes use of the RSA algorithm with a key length of 1024 or 2048 bits and a validity period of up to 7 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 CPS.

The Cybertrust key generation is carried out using an algorithm recognized as being fit for the purposes of certificates. Cybertrust uses RSA SHA-1.

Cybertrust Certification Practice Statement

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

6.1.3 Cybertrust Key Generation Audit (EV Guidelines)

For root keys generated after the release of EV Guidelines, Cybertrust Qualified Auditor witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the CA root keys produced. The Qualified Auditor then issues a report opining that the CA, during its root key and certificate generation process:

- Documented its Root CA key generation and protection procedures in its Certificate Policy , version, date and its Certification Practices Statement, version, date (CP and CPS);
- Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
- Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script; and
- Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- A video of the entire key generation ceremony may be recorded for auditing purposes.

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 device.

6.2.1.1 Cybertrust 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 device to store its private keys meeting the appropriate requirements of ISO.

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

6.2.2.1 Cybertrust 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.

Cybertrust Certification Practice Statement

6.2.2.2 Cybertrust CA Key Back Up

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

6.2.2.3 Secret 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.

6.2.2.4 Acceptance of Secret Shares

A secret shareholder receives the secret share within a physical medium, such as a Cybertrust CA approved hardware cryptographic module..

6.2.3 Cybertrust CA Public Key Distribution

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 CA to the browser manufacturers for inclusion in browser updates.

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 (FIPS 140-1 level 3 as minimum), 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.

Cybertrust Certification Practice Statement

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.

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 user 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 maintains a high-level network of systems security including firewalls. Network intrusions are detected. In specific:

Cybertrust Certification Practice Statement

- 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.

6.9 Time-stamping

Not applicable.

7. Certificate and CRL Profiles

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

7.1 Certificate Profile

Cybertrust certificate profiles are available upon request.

7.2 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.

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 separate terms and conditions 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 may subject to compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS and certain accreditation schemes it seeks to obtain and/or maintain compliant status.

8.1 Compliance Audit And Other Assessment

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

During the period in which it issues SureServer EV certificates, Cybertrust shall perform self audits as required by the EV Guidelines..

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 CPS.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CPS.
- Adherence to relevant laws.
- Asserting agreed service levels.
- Inspection of audit trails, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

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 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 Certification Practice Statement

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 CPS as described in this section.

9.1 Fees

The issuance and management of Cybertrust CA certificates is, in general, subject to payment of fees as announced on the Cybertrust web site cybertrust.omniroot.com or through requested quotes.

9.1.1 Refund policy

In general, having regard to the unique character of a certificate, Cybertrust does not accept requests for refund.

9.2 Financial Responsibility

Cybertrust maintains sufficient resources to meet its perceived obligations under this CPS. The Cybertrust CA makes this service available on an "as is" basis. Warranties are provided and liability is accepted to the extent explicitly set forth in the relevant agreements entered into with Cybertrust (such as, for example, the subscriber agreement). All other warranties and liabilities are disclaimed to the maximum extent permitted by applicable law.

9.3 Confidentiality of Business Information

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

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation or suspension of a 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:

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

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. Cybertrust may require that such parties enter into a confidentiality undertaking or similar form of security agreement.

Cybertrust Certification Practice Statement

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under , for example, the following conditions:

- 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.

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 certain 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

The 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 maintains a Privacy Policy which can be consulted at <http://cybertrust.omniroot.com/repository.cfm>.

9.5 Intellectual Property Rights

The Cybertrust CA 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 CPS.

The Distinguished names of all CAs of the Cybertrust CA, remain the sole property of Cybertrust.

Certificates are and remain property of the Cybertrust CA. The Cybertrust CA permits the reproduction and distribution of certificates on a non-exclusive 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, prior written permission of the Cybertrust CA.

The Cybertrust CA owns and reserves all intellectual property rights associated with its own products and services.

9.6 Representations and Warranties

Unless otherwise provided in this CPS in connection with the EV guidelines, warranties and representations shall be as set forth in the applicable agreement entered into by or with Cybertrust

Cybertrust Certification Practice Statement

regarding its certificate services (such as, for example, the subscriber agreement). Subscriber Obligations

Unless explicitly stated otherwise in this CPS or in the subscriber agreement, 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 CPS and associated policies published in the Cybertrust CA Repository.
- Refraining from tampering with a Cybertrust CA certificate.
- Using Cybertrust CA certificates for legal and authorised purposes in accordance with this CPS.
- Notifying Cybertrust CA or a Cybertrust RA of any changes in the information submitted.
- Ceasing to use a Cybertrust CA certificate if any featured information becomes invalid.
- Ceasing to use a Cybertrust CA certificate when it becomes invalid.
- Removing a Cybertrust CA certificate when invalid from any applications and/or devices they have been installed on.
- Using a Cybertrust CA 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 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 CA certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.

9.6.1 Relying Party Obligations

Unless explicitly stated otherwise in this CPS, each party relying on a Cybertrust CA certificate shall:

- Have the technical capability to use digital certificates.
- Receive notice of the Cybertrust CA and associated conditions for relying parties.
- Validate a Cybertrust CA 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 CA 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 CA 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.
- Verify the validity, suspension 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 CPS.
- Take any other precautions prescribed in the subscriber agreement, Cybertrust certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

Cybertrust Certification Practice Statement

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.

9.6.1.1 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 implied to be governed by the conditions set out in Cybertrust policy framework instigated by the Cybertrust CP and the Cybertrust CPS.

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

9.6.2 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.

9.6.3 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 CPS and any other conditions of usage that Cybertrust may make available. Parties demonstrate acceptance of the conditions of usage of the CPS 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. The Cybertrust CA Repositories include or contain:

- Information provided as a result of the search for a digital 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.
- If a repository becomes aware of or suspects the compromise of a private key, it will immediately notify the appropriate RA. The party that operates a Repository has exclusive responsibility of all acts or omissions associated with it.

The Cybertrust CA maintains a certificate repository during the application period and for a maximum of ten 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.

Cybertrust Certification Practice Statement

9.6.3.1 Reliance 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 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.

9.6.3.2 Accuracy of Information

The Cybertrust CA makes reasonable efforts to ensure that parties accessing its repositories receive accurate, updated and correct information.

9.6.4 Cybertrust CA Obligations

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

- Comply with this CPS and its amendments as published under <http://cybertrust.omniroot.com/repository>.
- 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 CPS and fulfil its obligations presented herein.
- Revoke certificates issued according to this CPS upon receipt of a valid and authenticated request to revoke a certificate from an RA.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Publish CRLs and/or OCSP responses of all suspended and revoked certificates on a regular basis in accordance with this CPS.
- Provide appropriate service levels according to a service agreement.
- Notify relying parties of certificate revocation by publishing CRLs on the Cybertrust CA repository.

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

- Any use of certificates, other than specified in this CPS.
- 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.

Cybertrust Certification Practice Statement

- 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.

The Cybertrust CA has no further obligations under this CPS.

9.6.5 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 CPS.
- Carry out all verification and authenticity actions prescribed by the Cybertrust CA procedures and this CPS.
- 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 CPS.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CPS.

9.6.6 Information incorporated by reference into a digital certificate

The following information is incorporated by reference in every digital certificate it issues:

- Terms and conditions of the Cybertrust CA CPS.
- 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.

The following information is also incorporated by reference in every SureServer EV digital certificate it issues:

- The CA/Browser Forum Guidelines for Extended Validation Certificates.

9.6.7 Pointers to incorporate by reference

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

Cybertrust Certification Practice Statement

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties, without prejudice to any further limitations set forth in any applicable agreement (such as, for example, a subscriber agreement).

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 CPS (in particular, products issued under the Guidelines for Extended Validation Certificates) 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 CPS.
- 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 is limited to the maximum extent permitted by applicable law and further in accordance with the limits set forth in the applicable agreement.

Notice is hereby given that a Cybertrust certificate must not solely be relied upon for transactions involving a monetary value exceeding the following limits:

SureCredential Personal Certificates	\$5000
SureCredential Professional Certificates	\$5000
SureServer Certificates	\$100000
SureCodesign Certificates	\$100000
SureServer EV Certificates	cf. section 9.8.1
SureServer EDU Certificates	0

9.8.1 Limitations on SureServer EV Certificate Liability

- (1) Subscribers and Relying Parties

Cybertrust Certification Practice Statement

In cases where Cybertrust has issued and managed SureServer EV certificates or any other product in compliance with the EV Guidelines, Cybertrust shall not be liable to the SureServer EV Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such certificate beyond those specified in the CA's EV Policies.

In cases where Cybertrust has not issued or managed the Certificate in complete compliance with the EV Guidelines, Cybertrust may seek to limit its liability to the Subscriber and to Relying Parties for any cause of action or legal theory involved for any and all claims, losses or damages suffered as a result of the use or reliance on such SureServer EV certificate, provided that all such purported limitations must also be specified in Cybertrust CPS, and provided further that in no event shall Cybertrust seek to limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than \$2,000 per Subscriber or Relying Party per Sure Server certificate.

(2) Indemnification of Application Software Vendors

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, Cybertrust acknowledges that the Application Software Vendors who has a root certificate distribution agreement in place do not assume any obligation or potential liability of Cybertrust under these Guidelines or that otherwise might exist because of the issuance or maintenance of Sure Server certificates or reliance thereon by Relying Parties or others.

Thus, Cybertrust shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to a SureServer EV Certificate, regardless of the cause of action or legal theory involved.

This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to a SureServer EV certificate issued by Cybertrust where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy a SureServer EV certificate this is still valid, or displaying as trustworthy: (1) a SureServer EV certificate that has expired, or (2) a SureServer EV certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the browser software either failed to check such status or ignored an indication of revoked status).

9.9 Indemnities

This section contains the applicable indemnities and apply without prejudice to any additional indemnification obligations set forth in any applicable agreement (such as, for example, a subscriber agreement).

To the extent permitted by law the subscriber must 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 Cybertrust may incur as a result of:

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

9.10 Term and Termination

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

Following publications, changes become applicable 30 days thereafter.

Cybertrust Certification Practice Statement

9.11 Individual notices and communications with participants

The Cybertrust CA accepts notices related to this CPS 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.

9.12 Amendments

Changes to this CPS are indicated by appropriate numbering.

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) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with art. 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 CPS the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:

J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel.: +32-47-733 82 96, Fax: + 32-16-32 54 38.

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Cybertrust digital certificates or other products and services. The law of Belgium apply

Cybertrust Certification Practice Statement

also to all Cybertrust commercial or contractual relationships in which this CPS 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 Leuven, 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.

9.16 Miscellaneous Provisions

9.16.1 Survival

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

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 CPS 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

APPLICATION SOFTWARE VENDOR: A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.

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 Class 3 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 verifying 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.

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 be 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

Cybertrust Certification Practice Statement

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 provide 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 subject 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.

ENTERPRISE EV CERTIFICATE: An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels that contain the domain that was included in an original Valid EV Certificate issued to the Enterprise RA.

ENTERPRISE RA: The Subject of a specified Valid EV Certificate that is authorized by the issuing CA to perform the RA function and authorize the CA to issue additional EV Certificates at third and higher domain levels that contain the domain that was included in the original EV Certificate, in accordance with the requirements of these Guidelines.

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.

GOVERNMENT ENTITY: A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

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

Cybertrust Certification Practice Statement

incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

INCORPORATING AGENCY: In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private Organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.

JURISDICTION OF INCORPORATION: In the case of a Private Organization, the country and (where applicable) the state or province where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

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 CPS.

NOTIFY

To communicate specific information to another person as required by this CPS 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.

PLACE OF BUSINESS: The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted

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.

REGISTERED AGENT: An individual or entity that is both:

authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (a) above.

REGISTERED OFFICE: the official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and legal notices received.

REGISTRATION NUMBER: The unique number assigned to the Private Organization Applicant or Subject entity by the Incorporating Agency in such entity's Jurisdiction of Incorporation.

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.

Cybertrust Certification Practice Statement

SECRET SHARE HOLDER

An person that holds a secret share.

SHORT MESSAGE SERVICE (SMS)

A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.

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.

SUBORDINATE CA: Certification authority whose certificates are signed by the Root CA, or another Subordinate CA. A Subordinate CA may issue EV Certificates if the appropriate EV OID(s) or the special any Policy OID is specified in the certificatePolicies extension.

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 CPS.

CYBERTRUST CA PROCEDURES

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

WEBTRUST EV PROGRAM: The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

WEBTRUST PROGRAM FOR CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at <http://www.webtrust.org/certauth fin.htm>.

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
RA: Registration Authority
LRA: Local Registration Authority
CEN/ISSS: European Standardisation Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
GSCA: 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