Certification Practice Statement

for Cybertrust Certification Services

Table of Contents

Document History

Document Change Control

	!" #	$ %&	' (
	) #	$ %&	% % !
	* +,- #	$ (('.	% % !-
	# !/ #	$ %&	[redacted]
	[redacted]		

[redacted]

- 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.

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 no

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:

(' '	
(' ' 7 $	(8
$ 7 .	
$ 7 . 9	
$ 7 .	
$.:	
/ $ $ /&. $	$&

* 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 certif

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.

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 otherwiselegitimate 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 58(s)23.807(m)]TJ 244.8 7.71368(l)-16.093.8095(t)-7.71368(r)-vcn53( )-31.52323dh5232(o)8.38216(r)23

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.

9 Cybertrust verifies by checking copy of verification method and payment.

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.

[redacted]

1.5.4 Certificate Profile

1.5.5 Documents Submitted to Identify the Applicant

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.

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 receiptcen rtice t arrcE38071(u)8.38216(s)23.8095(t)-16(1368(c5(t)-16(136)/332787(d)8.38071(d)8.32)23.8095(t)-)8.3

·tepr2(h)8.38216(n)8.3821C232(a)8.38071(p)8.388216(e)24

.

.

[redacted]

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 thesepe se t6(es)8A:3821

bbotle.1378

ob(on)8.382

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

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 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

[redacted]

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

- 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

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 enrols 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

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 Cybertrus

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.

Al1902( )-7.71368(t)-7.6.095d7(m)-24.14S2( )-7.71368(t)-7.6.095d7(m)-24.14S2( )-7.7 [(p)8.36(p)8.3838071( )-7.7144

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 polices etc. Howe

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 .
- 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'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
n Td ( )Tj T*[(I)-7.71441(n)8.38071(y88.38216(c)23.8095(t)-3327(o)32.1917(f)-7.71368( )278]TJ -258 -11.52 Td [(n Td

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 0-5.41424(u)4. 16(p)8.38216(p)8.382171(r)-0.

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 t

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

[redacted]

The Cybertrust CA might posts 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 ow

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 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 correspondance 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.

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.

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.

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,

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 Cyber

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 do

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 foce32(o)8a71433(d)-16 -11.52 Tdutybe

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:

- 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

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

[redacted]

[redacted]

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.

cert0958(y)-118.38216(fi(c)28.38071(l)-m(t)-7.71368(e)8.38216(e)8. 2(m)].216(n)8.38216(ce)8.38216

- 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.

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:

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

9.11 Individual notices and communications with par ticipants

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 Dcknoe Rm T R .52328(i)-16.093.ree diuiofaragiu t s
the other TC8812 4(r)-31.5232()23.8095(t)-7.71368(.52382)-16(u)8.3280.96( )31.5232(a)32.1917(i)-16.0958(s)23.8095(

also to all Cybertrust commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Cybertrust prod

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 d

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-timestampon o a

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