verizonbusiness
Security Solutions powered by Cybertrust

CA Certificate Policy

for Cybertrust Certification Services

Date: September 11, 2007

Version: v.2.3

[redacted]

5.3.3 Retraining Period and Retraining Procedures 22
5.3.4 Sanctions against Personnel 22
5.3.5 Controls of independent contractors 22
5.3.6

[redacted]

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

1.1 Overview

This CP applies to the specific domain of the Cybertrust CA that address the management of top level or root certificates issued under Cybertrust's own procedures. The purpose of this CP is to present the Cybertrust practices and procedures in managing certificates and to demonstrate sss.compliance with requirements pertaining to t

- Are issued by Cybertrust to a third party CA that meets the contractual and policy requirements of Cybertrust Omniroot services with regard to operational practices and technical implementation.
- Are issued to CAs only.

1.1.2 Certificate usages

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

Any other use of Cybertrust Omniroot and Omniroot certificates is forbidden.

1.2 Document Name and Identification

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

The identifiers for the certificate policies specified in this CP will be determined at a later stage.

1.3 PKI participants

1.3.1 Cybertrust Certification Authority

A Certification Authority is an organisation that issues digital certificates that are used in the public domain or within a business or transactions context. Cybertrust is a Certification Authority.

The Cybertrust CA ensures the availability of all services pertaining to the management of

The Cybertrust CA Root has been used to certify each of the private keys of the subsequent third party CA roots. By validating the certificate of such a CA, trust vested in Cybertrust can also be extended to the certified third party CA root.

1.3.2 Cybertrust Registration Authorities

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

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

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

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

The Cybertrust RA acts locally on approval and authorisation by the Cybertrust CA. The Cybertrust RA acts in accordance with the approved practices and procedures of the Cybertrust CA including this CP and documented Cybertrust RA procedures.

Sometimes to grant a specific certificate type, Cybertrust RAs might rely on certificates issued by third party certification authorities or other third party databases and sources of 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 Cybertrust RAs.

1.3.3 Subscribers

Subscribers of Cybertrust Omniroot are third party CAs that seek to be issued with certificates within a hierarchy managed by Cybertrust.
Subscribers of Cybertrust services are also natural or legal persons that successfully apply for a CA 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.

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

Subscribers legal persons which are natural persons, are conditionally accepted as subscribers for CA chaining services. The relationship of these persons with the CA to be chained to has to

[redacted]

1.4 Certificate use

Certain limitations apply to the use of Cybertrust CA certificates.

1.4.1 Appropriate certificate usage

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

- Authentication
- Assurance about the identity of a remote device

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

1.4.2 Prohibited certificate usage

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

1.4.3 Certificate extensions

Cybertrust root certificate extensions are defined by the X.509 v.3 standard other standards as well as any other formats including those used by Microsoft and Netscape.

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. Cybertrust pro-actively supports and participates in the proliferation of industry, government or other certificate policies for its public certificates as it sees appropriate.

1.4.4 Critical Extensions

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

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

1.5 Policy Administration

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

[redacted]

3. Identification and Authentication

Cybertrust maintains documented practices and proce

- Subscriber certificate requests are complete, accurate and duly authorized.

In particular:

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

3.3.1 Documents used for authentication

d=54Thes03563(l)3.69012(i)3.-21.8837(a)3.80613(r)-0.884125(t)-

[redacted]

4. Certificate Life-Cycle Operational Requirements

All entities within the Cybertrust domain including third party CAs, RAs and subscribers or other participants, have a continuous duty to inform the Cybertrust CA of all changes in the information

4.6.1.2 Certificate Life-Cycle Operational Requirements

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

4.6.1.3Reliance at Own Risk

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

4.6.2 Relying party

The duties of a relying party are as follows:

4.6.2.1Relying party duties

A party relying on a certificate will:

- Receive notice of the Cybertrust CA and associated conditions for relying parties.
- Validate a Cybertrust CA 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.
- 61-0.82769(ua)0.292471(l)-5.749(t)-4.40

Subject to prior agreement with Cybertrust any Cybertrust RA may carry out the identification and authentication of holders seeking to revoke a certificate.

Revocation requests can also be placed directly to the Cybertrust RA at: Cybertrust, Philipssite 5, 3001, Leuven, Belgium or MIDsupport@cybertrust.com.

Upon request from an RA, the Cybertrust CA revokes the CA 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

5. Management, Operational, And Physical Controls

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

5.1 Physical Security Controls

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

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

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

Physical access is restricted by implementing 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.

The Cybertrust CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

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

- Misrepresentations by the candidate.
- Any other as it might be deemed necessary.

5.3.2 Training Requirements and Procedures

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

5.3.3 Retraining Period and Retraining Procedures

Periodic training updates might also be performed t

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.

Auditing events are not given log notice.

5.5 Records Archival

Cybertrust CA keeps internal records of the following items:

- CA certificates for a period of a maximum of 10 years after the expiration of the certificate.
- Audit trails on the issuance of CA certificates for a period of 5 years after issuance of a certificate.
- Audit trail of the revocation of a CA certificate for a period of 5 years after revocation of a certificate.
- CRLs for a minimum of 5 year after expiration or revocation of a CA certificate.
- Support documents on the issuance of CA certificates for a period of 5 years after expiration of a certificate.

Cybertrust CA keeps archives in a retrievable format.

5.5.1 Types of records

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

5.5.2 Retention period

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

5.5.3 Protection of archive

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

- 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.

[redacted]

6.2.1 Cybertrust CA Key Generation Devices

The generation of the private keys of the Cybertrus

[redacted]

6.5 Activation Data

[redacted]

8. Compliance Audit and Other Assessment

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

[redacted]

[redacted]

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

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

9.6.1 Subscriber Obligations

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

- Having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with the Cybertrust CA.
- Ensuring that the public key submitted to the Cybertrust CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the Cybertrust CA CP and associated policies published in the Cybertrust CA Repository.
- Refraining from tampering with a Cybertrust CA certificate.
- Using Cybertrust CA certificates for legal and authorised purposes in accordance with this CP.
- Notifying Cybertrust CA or a Cybertrust RA of any changes in the information submitted.
- Ceasing to use a Cybertrust CA certificate if any becomes invalid.
- Removing Cybertrust CA certificate when from applications and devices they have been installed according to policy.

- Inaccuracy or changes to the certificate content, as notified to the subscriber.

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

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

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

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

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

- Any use of certificates, other than specified in this CP.
- Falsification of transactions.
- Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving certificates.
- Compromise of private keys associated with the certificates.
- Loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates.
- The submission of erroneous or incomplete data from an RA, including identification data, serial numbers and public key values.
- Erroneous or incomplete requests for operations on certificates by the RA.
- Acts of God.
- The use of certificates.
- The use of public or private keys of cross-certified (non-subordinate) CA's and their relying parties.
- Services delivered to any subscriber that maintains a CA chaining relationship within its own organisation with another certification authority. This limitation applies to the services delivered to the whole customer organisation and not just specific root or

- Receive, verify and relay to the Cybertrust CA all requests for revocation of a Cybertrust CA certificate in accordance with the Cybertrust CA procedures and the Cybertrust CA CP.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CP.

9.6.7 Information incorporated by reference into a digital certificate

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

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

9.6.8 Pointers to incorporate by reference

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

9.7 Disclaimers of Warranties

This section includes disclaimers of express warr80613( )-4(.)8.32394(5D)-2.7801aby9.ar

9.8 Limitations of Liability

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

Further information can be found at:
http://cybertrust.omniroot.com/repository.

9.9 Indemnities

This section contains the applicable indemnities.

9.9.1 Indemnity

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

- Failure to protect the subscriber's private key,
- 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 CP remains in force until notice of the opposite is communicated by the Cybertrust CA on its web site or repository.

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

9.11 Individual notices and communications with participants

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

9.12 Amendments

Changes to this CP are indicated by appropriate numbering.

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

9.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify Cybertrust sm ye dipute wit view to e

Uwpon receipt o iput Nice, Cybertrust 1.5567(i)3.69012tfte tha ie

Cybertrust Dispute m1.18283(a)-21.6892(n)3.80456(a)3.80456(g)e 9.03720(e

ithin two (2) business days (m)6.5311 5567( )p11.4681(r)-14.5726(e)c.1

micepatentiol atcmp11.18681(e)-9.03563(m)-1.71495(b)-9.03563(e)3.80613(r)-0.87.

mnagemn and ecurity of1.7151781fticer h counel or at rtetion ofice

9.16 Miscellaneous Provisions

9.16.1 Survival

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

9.16.2 Severability

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

.

10. List of definitions

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.
ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.
APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to a CA to issue a digital certificate.
ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.
ASSURANCES
A set of statements or conduct aiming at conveying a general intention.
AUDIT
Procedure used to validate compliance with formal criteria or controls.

[redacted]

11. List of acronyms

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