GlobalSign CA Certificate Policy

Date: May 12th 2009

Version: v.3.4

Table of Contents

Document History

Distribution List

Version	Company	Name + Title	Action
V2.0	30.06.05	Andreas Mitrakas	Second version
V2.1	26.1.07	Johan Sys	Distributed to Policy Board
V2.2	19.6.07	Johan Sys	Distributed to Policy Board
V2.3	14.11.07	Steve Roylance	Distributed to Policy Board
V3.0	17.12.07	Steve Roylance	Distributed to Policy Board
V3.1	18.04.08	Steve Roylance	Distributed to Policy Board
V3.2	05.12.08	Steve Roylance	Distributed to Policy Board
V3.3	11.02.09	Steve Roylance	Distributed to Policy Board
V3.4	12.05.09	Steve Roylance	Distributed to Policy Board

Document Change Control

Version	Release Date	Author	Status + Description
V3.0	17.12.07	Steve Roylance	Administrative update
V2.3	14.11.07	Steve Roylance	Administrative update
V 2.2	19.6.07	Johan Sys	Small administrative update
V 2.1	26.1.07	Johan Sys	Added GlobalSign Root CA R2
V2.0	30.06.05	Andreas Mitrakas	Second version
1.1.1	05.09.05	Jean-Paul Declerck	Final version
V3.0	17.12.07	Steve Roylance	Final Version
V3.1	20.05.08	Steve Roylance	Modification of RootSign to TrustedRoot
V3.2	16.12.08	Steve Roylance	Registered GlobalSign Logo and removal of suspension.
V3.3	11.02.09	Steve Roylance	Support for TrustedRoot TPM
V3.4	15.05.09	Steve Roylance	Administrative update

Acknowledgments

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

- CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements
- CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 5280: 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 101 456: Policy requirements for certification authorities issuing qualified certificates.
- 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

The above quoted CWA 14167-1 and CWA 14167-2 have been published in a Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council

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

- AICPA/CICA, WebTrust Program for Certification Authorities.
- AICPA/CICA, WebTrust For Certification Authorities – Extended Validation Audit Criteria.

This CP intends to become compliant with the requirements of the above-mentioned scheme. The dates of compliance will be announced on the web site of GlobalSign.

2. Introduction

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

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

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

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

GlobalSign NV
attn. Legal Practices,
Ubicenter,
Philipssite 5
B-3001 Leuven,
Belgium.
Tel:+ 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

The GlobalSign CA operates within the scope of activities of GlobalSign NV/SA. This CP addresses the requirements of the CA that issues top level certificates. Top-level certificates are also known as root certificates or anchor certificates. The GSCA also issues other certificate types at varying levels of its hierarchy. More information can be obtained from http://www.globalsign.com/repository.

This CP applies in all cases of offline solutions that are associated with the CA chaining services that GlobalSign makes available. This CP also applies in cases related with the validation of the certificate path for certificates that are issued at lower levels in it’s the GlobalSign hierarchy like for example end entity certificates.

This CP is final and binding between GlobalSign NV/SA, a company under public law, with registered office at Ubicenter, Philipssite 5, B-3001 Leuven, VAT Registration Number BE

0459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (Hereinafter referred to as "GlobalSign")

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the GlobalSign CA.

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

2.1 Overview

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

This CP sets out the objectives to identify the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of top-level root certificates of GlobalSign. This CP describes the policy requirements to issue, manage and use GlobalSign top-root certificates of GlobalSign. As a top root CA, GlobalSign manages a hierarchy of certificates according to publicised practices to be found under http://www.globalsign.com/repository.

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

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

In addition to the CP and Certificate Practice Statement, GlobalSign maintains a range of adjacent documented polices which include but are not limited to addressing such issues as:

- The GlobalSign Limited Warranty Policy that addresses issues on insurance.
- The GlobalSign Data Protection Policy on the protection of personal data
- Business continuity
- Security policy
- Personnel policies
- Key management policies
- Registration procedures
- etc.

A subscriber or relying party of a GlobalSign CA certificate must refer to the GlobalSign CP in order to establish trust on a certificate issued by the GlobalSign Root CA as well as for notices

with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the GlobalSign certificate hierarchy, including the Top Root CA and operational roots, which can be established on the basis of the assertions of this CP.

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

The exact name of the GlobalSign CA certificates that makes use of this CP is

- GlobalSign Root CA*
- GlobalSign Root CA - R2*
- GlobalSign Root CA - R3*

TrustedRoot** are the GlobalSign services which allow third-party CAs to chain to one of the GlobalSign CA certificates.

- GlobalSign Trusted Platform Module Root CA*

TrustedRoot TPM** is the GlobalSign services which allows third-party CAs to chain to one of the GlobalSign Trusted Platform Module Root CA certificates.

** They are called collectively the GlobalSign CA Root*
*** They are called collectively TrustedRoot*
Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data electronically. By means of a digital certificate, GlobalSign provides confirmation of the relationship between a named entity (subscriber) and its public key. For the purposes of this CP an end entity is a subscribing third party Certification Authority that seeks to enter the GlobalSign hierarchy. The purpose of entering the GlobalSign hierarchy enhances trust in the hierarchy as well as greater functionality within third party applications such as browsers etc. GlobalSign seeks to maintain a position of leadership with regard to inclusion of its top root in third party application. This endeavour does not undermine, however, the ability of GlobalSign to revise its approach and seek alternative strategies in the future. It is at the discretion of and a duty of the end entity that is a third party CA to assess the value of the GlobalSign services at any point in time and act accordingly.

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

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

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

This CP is made available on-line in the Repository of the issuing CA under http://www.globalsign.com/repository

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

2.1.1 GlobalSign TrustedRoot

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

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

2.1.2 Certificate usages

Certain limitations apply to the use of GlobalSign TrustedRoot and TrustedRoot 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 GlobalSign TrustedRoot and TrustedRoot certificates is forbidden.

2.2 Document Name and Identification

The identifiers under control of GlobalSign which refer to this document are.

1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy
1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy
1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy
1.3.6.1.4.1.4146.1.30	Time Stamping Certificates Policy
1.3.6.1.4.1.4146.1.40	Client Certificates Policy
1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy
1.3.6.1.4.1.4146.1.60	CA Chaining Policy
1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90	TrustedRoot TPM Policy
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy

2.3 PKI participants

2.3.1 GlobalSign 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. GlobalSign is a Certification Authority. Sometimes, a certification authority is also described by the term issuing authority.

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

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

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

Root certificates can be used for any public purposes. As “public”, this CP considers any use that takes place among CAs that is not restricted to uses governed by voluntary agreements under

private law among participants. Closed user groups are also permitted to leverage on the GlobalSign hierarchy.

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

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

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

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

- Issuance
- Revocation
- Renewal
- Status validation
- Directory service

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

2.3.1.1 GlobalSign outsource agent

GlobalSign relies on outsource agents to operate a secure facility and deliver CA services including the issuance, revocation, renewal and status validation of GlobalSign CA certificates. The GlobalSign outsource agent operates a service to GlobalSign on the basis of a service agreement.

2.3.1.2 Roles of GlobalSign

GlobalSign 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 GlobalSign.

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

The main activities of GlobalSign are to:

- Manage an international network of RAs, establishing the brand name of GlobalSign as a universal Trusted Third Party leveraging on in PKI technology.
- Manage the life cycle of digital certificates issued to end user entities as well as to other certification authorities and administrators within the GlobalSign domain.

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

2.3.1.3 GlobalSign root and hierarchy

GlobalSign makes available to subscribers a dedicated root hierarchy to ensure the integrity of the end user certificate and the uniqueness of the resources that it makes available. The GlobalSign CA Root belongs to the broader domain of the GlobalSign 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 GlobalSign etc. as well as other participating CAs that take advantage from GlobalSign's root, which is embedded in applications. This GlobalSign Certificate Policy addresses the Root level of the GlobalSign hierarchy and provides guidance with regard to the general conditions of the GlobalSign services.

The GlobalSign 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 GlobalSign can also be extended to the certified third party CA root.

2.3.2 GlobalSign Registration Authorities

The GlobalSign CA reaches its subscribers through a designated Registration Authorities. An RA requests the issuance 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 GlobalSign RA interacts with the subscriber to deliver public certificate management services to the end-user. A GlobalSign RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to GlobalSign CA certification services.
- Attends all stages of the identification of subscribers as assigned by the GlobalSign 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 GlobalSign CA to issue a certificate.
- Initiates the process to revoke a certificate and request a certificate revocation from the GlobalSign CA.

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

Sometimes to grant a specific certificate type, GlobalSign 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 GlobalSign 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 GlobalSign RAs.

2.3.3 Subscribers

Subscribers of GlobalSign TrustedRoot are third party CAs that seek to be issued with certificates within a hierarchy managed by GlobalSign.
Subscribers of GlobalSign services are also natural persons or legal persons that successfully apply for a CA certificate. Subscribers use electronic signature services within the domain of the GlobalSign. Subscribers are parties that:

- Set the framework of providing certification services with the GlobalSign 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 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 be duly explained and justification must be provided to GlobalSign. If representation of a third party is desired, GlobalSign recommends alternative credentials might be required (e.g. attribute or role certificates), which, however, can be arranged on a case-by-case basis.

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. Additional identification of the applying organisation is also needed.

2.3.4 Subjects

Subjects of GlobalSign TrustedRoot are third party CAs that seek to be issued with certificates within a hierarchy managed by GlobalSign

Subjects of GlobalSign CA certificates services may be natural persons themselves or they may be associated with a subscriber through a contractual obligation on the 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 GlobalSign RA or a Service Provider that requires it to use a certificate within the designated service. A subject nominates a named Certificate Applicant also called a Subscriber, to apply for a certificate. A certificate applicant can be any natural person acting on behalf of the subject.

Subjects of GlobalSign CA root certificates are the same as the applying organisation, which is the third party CA that requests GlobalSign for CA chaining services.

2.3.5 Certificate Applicants

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

- Applying for a certificate.
- Agreeing with and accepting the 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.

2.3.6 Relying Parties

Relying parties are natural persons 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 GlobalSign operators that receive signed requests from GlobalSign CA subjects are relying parties of the GlobalSign certificates.

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

2.4 Certificate use

Certain limitations apply to the use of GlobalSign CA certificates.

2.4.1 Appropriate certificate usage

Root certificates issued under the GlobalSign 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 GlobalSign CA certificates may result in an annulment of warranties offered by the GlobalSign CA to subscribers and relying parties.

2.4.2 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.

2.4.3 Certificate extensions

GlobalSign 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.

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

2.4.4 Critical Extensions

GlobalSign 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.

2.5 Policy Administration

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

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

2.5.1 Scope

In an effort to invoke credibility and Trust in the publicised GlobalSign CP and to better correspond to accreditation and legal requirements, GlobalSign may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CP and/or CP.

2.5.2 GlobalSign Policy Management Authority

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

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

The Management member chairs the GlobalSign Policy Management Authority ex officio.

All members of the GlobalSign 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 GlobalSign Policy Management Authority counts double.

2.5.3 Acceptance of Updated Versions of the CP

Upon approval of a CP update by the GlobalSign Policy Management Authority that CP is published in the GlobalSign online Repository at http://www.globalsign.com/repository.

GlobalSign publishes a notice of such updates on its public web site at http://www.globalsign.com. The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CP is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the GlobalSign CP.

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

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

2.5.3.1 Changes with notification

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

2.5.4 Version management and denoting changes

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

- Minor editorial corrections
- Changes to contact details

2.6 Definitions and acronyms

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

3. Publication and Repository Responsibilities

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

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

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

GlobalSign refrains from making publicly available certain elements of documents including security controls, procedures, internal security polices etc. However these elements are disclosed in audits associated with formal accreditation schemes that GlobalSign adheres to.

3.1 Access control on repositories

While GlobalSign 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.

4. Identification and Authentication

GlobalSign maintains documented practices and procedures to authenticate the identity and/or other attributes of an end-user certificate applicant to a GlobalSign CA or GlobalSign RA prior to issuing a certificate.

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

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

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

4.1 Naming

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

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

GlobalSign does not accept trademarks, logos or otherwise copyrighted graphic or text material for inclusion in its certificates.

4.2 Initial Identity Validation

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

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

GlobalSign accepts other CAs wishing to enter its own network and operate under its own hierarchy. Following an initial assessment and the signing of a specific agreement with GlobalSign the applicant CA has to provide GlobalSign with certain identification documents including an authorisation letter, articles of association. GlobalSign retains its right to consult third party databases that identify organisations in this regard.
CA chaining services do not require the physical appearance of the customer as long as an agreement between the applicant organisation and GlobalSign has been executed.

4.3 Subscriber registration process

GlobalSign ensures that:

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

In particular:

- GlobalSign provides notice to the applicant through its web site at http://www.globalsign.com and the dedicated policy framework published on its repository at http://www.globalsign.com/repository .

- Before entering any contractual relationship with the subscriber, GlobalSign makes available a CA chaining agreement, which the applicant must approve prior to placing a request with GlobalSign.
- GlobalSign's policy framework is limited under data protection and consumer protection laws and warranty, as explained in this GlobalSign CP as well as GlobalSign's Limited Warranty framework.
- GlobalSign maintains documented contractual relationships with all third party registration authorities or outsourced agents it uses to deliver certificates.

4.3.1 Documents used for subscriber registration

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

4.3.2 Data needed for subscriber registration

For CA chaining services, evidence requires might include:

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

4.3.3 Pseudonyms

Pseudonyms are not permitted for GlobalSign TrustedRoot certificates.

4.3.4 Records for subscriber registration

GlobalSign 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.

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

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

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

4.4 Identification and Authentication for Revocation Requests

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

5. Certificate Life-Cycle Operational Requirements

All entities within the GlobalSign domain including third party CAs, RAs and subscribers or other participants, have a continuous duty to inform the GlobalSign 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 GlobalSign CA issues, revokes certificates following an authenticated and duly signed request issued by a GlobalSign RA.

To carry out its tasks, GlobalSign relies on third party agents. GlobalSign, however, assumes responsibility and accountability towards all entities in its domain as well as relying parties, for acts or omissions of all third party agents it may use to deliver services associated with CA operations within the GlobalSign CA.
Certificate Application

5.1 Certificate Application for a root certificate

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

5.2 Certificate Application Processing

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

The RA uses documented procedures and adopts its own practices.

5.3 Certificate Issuance

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

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

Issued certificates are delivered to the subject.

5.4 Certificate generation

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

- The procedure to issue a certificate including a root certificate is securely linked to the associated registration and certificate renewal, including the provision of any subscriber generated public key.
- GlobalSign ensures the uniqueness of the distinguished name assigned to the subscriber within its own domain.
- The confidentiality and integrity of registration data is ensured at all times through appropriate means.
- The authentication of RA registrars is ensured through appropriate credentials.

- Certificate requests and generation are also supported by robust and tested procedures.
- If external registration service providers are used, registration data is exchanged with authenticated registration service providers.
- GlobalSign accepts independent audits of its services and practices.

5.5 Certificate Acceptance

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

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

The GlobalSign CA publishes issued certificates.

5.6 Key Pair and Certificate Usage

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

5.6.1 Subscriber

The obligations of the subscriber include the following ones:

5.6.1.1 Subscriber duties

The duties of subscribers include the following:

1. Accepting all applicable terms and conditions in the CP of GlobalSign published in the GlobalSign Repository.
2. Notifying the GlobalSign CA or a GlobalSign RA of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a GlobalSign CA certificate when it becomes invalid.
4. Using a GlobalSign CA certificate, as it may be reasonable under the circumstances.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
6. Using secure devices and products that provide appropriate protection to their keys and which were approved prior by GlobalSign.
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 GlobalSign or any GlobalSign directory any material that contains statements that violate any law or the rights of any party.
9. Request the revocation of a CA certificate in case of an occurrence that materially affects the integrity of a GlobalSign CA certificate.
10. Refraining from tampering with a certificate.
11. Only using certificates for legal and authorised purposes in accordance with the CP and the CA chaining agreement.

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

5.6.1.2 Certificate Life-Cycle Operational Requirements

Subscribers have a continuous duty to inform directly a GlobalSign 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.

5.6.1.3 Reliance at Own Risk

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

5.6.2 Relying party

The duties of a relying party are as follows:

5.6.2.1 Relying party duties

A party relying on a certificate will:

- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign CA certificate by using certificate status information (e.g. a CRL or OCSP) published by GlobalSign, 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 GlobalSign 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 GlobalSign certificate only as it may be reasonable under the circumstances.
- Trust a CA certificate only if it has not been revoked.
- Validate at least those certificate attributes that materially affect the relying party's own signature policy or practices.

5.6.2.2 GlobalSign CA Repository and Web site Conditions

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

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

5.7 Certificate Renewal

Renewal of GlobalSign CA certificates is not supported.

5.8 Certificate Revocation

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

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

Revocation requests can also be placed directly to the GlobalSign RA at: GlobalSign, Philipssite 5, 3001, Leuven, Belgium or ra@globalsign.com or through the telephone numbers provided in the introduction of this CP or via the revocation form in the GlobalSign Legal repository. www.globalsign.com/repository

Upon request from an RA, the GlobalSign 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 obligation under this CP or the CA chaining agreement.
- The performance of a person's obligations under this CP is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.

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

5.9 Certificate Status Services

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

5.10 End of Subscription

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

6. Management, Operational, And Physical Controls

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

6.1 Physical Security Controls

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

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

The GlobalSign 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 GlobalSign 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 GlobalSign CA implements a partial off-site backup.

The sites of the GlobalSign CA host the infrastructure to provide the GlobalSign CA services. The GlobalSign 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.

6.2 Procedural Controls

The GlobalSign 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 GlobalSign CA takes measures regarding 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.

GlobalSign may exercise vetting of personnel in trusted positions.

GlobalSign pursuits the accountability of all actors for actions performed.

The GlobalSign CA implements dual control for critical CA functions.

6.3 Personnel Security Controls

6.3.1 Qualifications, Experience, Clearances

The GlobalSign 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.

6.3.2 Training Requirements and Procedures

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

6.3.3 Retraining Period and Retraining Procedures

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

6.3.4 Sanctions against Personnel

GlobalSign 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.

6.3.5 Controls of independent contractors

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

6.3.6 Documentation for initial training and retraining

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

6.4 Audit Logging Procedures

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

GlobalSign CA audit records events that include but are not limited to

- Issuance of a certificate
- Revocation of a certificate
- Published CRL s

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.

GlobalSign 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 GlobalSign 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.

6.5 Records Archival

GlobalSign 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.

GlobalSign CA keeps archives in a retrievable format.

6.5.1 Types of records

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

6.5.2 Retention period

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

6.5.3 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.

6.5.4 Procedures to obtain and verify archive information

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

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

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

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

6.6 Compromise and Disaster Recovery

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

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

6.7 CA or RA Termination

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

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

7. Technical Security Controls

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

7.1 Key Pair Generation and Installation

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

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

7.1.1 GlobalSign CA Private Key Generation Process

The GlobalSign CA uses a trustworthy process for the generation of its root private key according to a documented procedure. The GlobalSign CA distributes the secret shares of its private key(s).

7.1.1.1 GlobalSign CA Private Key Usage

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

7.1.1.2 GlobalSign CA Private Key Type

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

For the operational CA keys it uses the GlobalSign CA makes use of the RSA algorithm with a key length of 2048 bits and a validity period of up to 14 years.

7.1.2 GlobalSign CA Key Generation

The GlobalSign 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 GlobalSign CA implements and documents key generation procedures, in line with this CP.

The key generation is carried out using an algorithm recognized as being fit for the purposes of issuing certificates. GlobalSign uses RSA SHA-1 and RSA SHA-256

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

7.2 Key Pair re-generation and re-installation

The GlobalSign 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.

7.2.1 GlobalSign CA Key Generation Devices

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

7.2.1.1 GlobalSign CA Key Generation Controls

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

7.2.2 GlobalSign CA Private Key Storage

The GlobalSign CA uses a secure cryptographic device to store its private keys meeting the appropriate requirements of ISO.

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

7.2.2.1 GlobalSign CA Key Storage Controls

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

7.2.2.2 GlobalSign CA Key Back Up

The GlobalSign 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.

7.2.2.3 Secret Sharing

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

7.2.2.4 Acceptance of Secret Shares

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

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

7.2.3 GlobalSign CA Public Key Distribution

Public key distribution of GlobalSign's own public key takes place according to GlobalSign's own practices as well as additional conditions required by Law in Belgium.

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

7.2.4 GlobalSign CA Private Key Destruction

GlobalSign 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.

7.3 Private Key Protection and Cryptographic Module Engineering Controls

The GlobalSign 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, 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.

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

7.4 Other Aspects of Key Pair Management

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

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

The GlobalSign 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 GlobalSign CA, the CA ensures that any agreement with the resource owner or services provider is compliant with the requirements for disaster recovery.

7.4.2 CA public key revocation

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

- Notify all CAs with which it is cross-certified.

7.4.3 CA private key is compromised

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

7.5 Activation Data

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

7.6 Computer Security Controls

The GlobalSign CA implements computer security controls.

7.7 Life Cycle Security Controls

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

7.8 Network Security Controls

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

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

8. Certificate and CRL Profiles

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

8.1 Certificate Profile

GlobalSign Certificates conform generally to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008.

Field	Value or Value constraint
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate – sha1RSA - in accordance with RFC 3279.
Issuer DN	GlobalSign together with the appropriate intermediate issuing CA appended to the description.
Valid From	Universal Coordinate Time base Synchronized to the Royal Observatory of Belgium. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinate Time base Synchronized to the Royal Observatory of Belgium. Encoded in accordance with RFC 5280.
Subject DN	In accordance with 3.1
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

8.1.1 Authority Key Identifier

GlobalSign generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

8.1.2 Authority Information Access

GlobalSign generally populates the Authority Information Access extension of X.509 Version 3 end user Subscriber Certificates and if appropriate Intermediate CA Certificates with the URL of the location where a Relying Party can obtain the issuing CA certificate. The criticality field of this extension is set to FALSE.

8.1.3 CRL Distribution Points

Most GlobalSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

8.1.4 Subject Key Identifier

Where GlobalSign populates X.509 Version 3 certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

8.1.5 Subject Alternative Name

Where GlobalSign populates X.509 Version 3 certificates with a subjectAlternativeName extension, the subjectAlternativeName is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

8.2 CRL Profile

Most GlobalSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

Field	**Value or Value constraint**
Version	V2 in accordance with RFC 5280.
Issuer DN	The Entity who has signed and issued the CRL
Effective date	Issue date of the CRL. CRLs are effective upon issuance.
Next update	Date by which the next CRL will be issued.
Signature Algorithm	Object identifier of the algorithm used to sign the certificate – sha1RSA - in accordance with RFC 3279.
Authority Key Identifier	160-bit SHA-1 hash of the public key of the CA issuing the Certificate
CRL Number	A monotonically increasing sequence number in accordance with RFC 5280
This update	Issuance
Next Update	Date of Issuance + 3 hours

8.3 OCSP Profile

The GlobalSign 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 GlobalSign CA, on request from parties explaining their interest.

8.4 Time Stamping Profile for Time Stamping Services

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

9. Compliance Audit and Other Assessment

The GlobalSign CA accepts under condition the auditing of practices and procedures it does not publicly disclose. The GlobalSign 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 GlobalSign CA accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CP and accreditation schemes it publicly claims compliance with.

9.1 Compliance Audit and Other Assessment

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

GlobalSign has successfully been audited and currently meets the requirements of the accreditation scheme known as WebTrust for CAs. GlobalSign seeks to maintain its accreditation.

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

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

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

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

9.1.1.1 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, GlobalSign may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. GlobalSign 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, GlobalSign remains ultimately in charge of the whole process. GlobalSign limits its responsibility thereof according to the conditions in this GlobalSign CP.

9.1.1.2 Secure Devices and Private Key Protection.

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

10. Other Business and Legal Matters

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

10.1 Fees

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

10.1.1 Refund policy

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

10.2 Financial Responsibility

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

10.3 Confidentiality of Business Information

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

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

The following items are not confidential information:

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

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

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

The GlobalSign may charge an administrative fee to process such disclosures.

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

10.3.1 Disclosure Conditions

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

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

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

The GlobalSign 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 GlobalSign CA encrypts all communications of confidential information including:

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

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

10.4 Privacy of Personal Information

GlobalSign CA makes available a specific Data Protection Policy for the protection of personal data of the applicant applying for a GlobalSign CA certificate that they make available through their web site. The GlobalSign CA adheres to the documented Data Protection Policy of GlobalSign NV available from http://www.globalsign.com/repository

The practices and operations of the GlobalSign CA are within the boundaries of the Belgian law of 8 December, 1992, on privacy protection in relation to the processing of personal data as modified by the law of 11 December 1998, implementing the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 p. 0031 – 0050).

The regulation on the protection of personal data in the Belgium implements the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

GlobalSign CA also acknowledges Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The GlobalSign CA operates within the conditions for the protection of personal data asserted in this CP.

GlobalSign CA has made appropriate representations before the Belgian Data Protection Commission with regard to the archives of personal data it maintains, collects and processes. The Belgian Data Protection Commission can be contacted by post at: Ministry of Justice, Waterloolaan 115, B-1000 Brussels, Belgium (tel. +32 2 5427206)

10.5 Intellectual Property Rights

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

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

Certificates are and remain property of the GlobalSign CA or the rightful owner that licenses certificate management over to GlobalSign. The GlobalSign CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of the GlobalSign CA.

The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.

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

10.6 Representations and Warranties

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

Participants that may make representations and warranties include GlobalSign CA, RAs, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the GlobalSign domain, including the GlobalSign 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.

10.6.1 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 GlobalSign CA.
- Ensuring that the public key submitted to the GlobalSign CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the GlobalSign CA CP and associated policies published in the GlobalSign CA Repository.
- Refraining from tampering with a GlobalSign CA certificate.
- Using GlobalSign CA certificates for legal and authorised purposes in accordance with this CP.
- Notifying GlobalSign CA or a GlobalSign RA of any changes in the information submitted.
- Ceasing to use a GlobalSign CA certificate if any featured information becomes invalid.
- Ceasing to use a GlobalSign CA certificate when it becomes invalid.
- Removing a GlobalSign CA certificate when invalid from any applications and/or devices they have been installed on.
- Using a GlobalSign 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 GlobalSign CA or any GlobalSign 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 GlobalSign CA certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.
- Submit accurate and complete information to GlobalSign in accordance with the requirements of this CP particularly with regards to registration.
- Only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber according to this CP or the executed CA Chaining agreement.
- Exercise absolute care to avoid unauthorized use of its private key.
- Generate subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures.

- Use a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.
- Notify GlobalSign without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The subscriber's private key has been lost, stolen, potentially compromised; or
    - Control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code)
      or
    - Inaccuracy or changes to the certificate content, as notified to the subscriber.

The subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and GlobalSign 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 GlobalSign seeks to ensure the trustworthiness of the relationship with the CA chaining subscriber. The subscriber refrains at all times from seeking CA chaining services by other certification authorities at the same time that it use the CA chaining services of GlobalSign. This limitation applies to the whole subscriber organization and not to the designated roots alone.

10.6.2 Relying Party Obligations

A party relying on a GlobalSign CA certificate promises to:

- Have the technical capability to use digital certificates.
- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign CA certificate by using certificate status information (e.g. a CRL) published by the GlobalSign CA in accordance with the proper certificate path validation procedure.
- Trust a GlobalSign 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 GlobalSign 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.

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

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

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

10.6.2.1 Conveying Relying party obligations

In order to give uninhibited access to revocation information and subsequently invoke Trust in its own services, GlobalSign 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 GlobalSign public services, however, the use of GlobalSign resources that relying parties make is implicitly governed by the conditions set out in GlobalSign’s policy framework instantiated by the GlobalSign CP.

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

10.6.3 Subscriber Liability towards Relying Parties

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

10.6.4 GlobalSign CA Repository and Web site Conditions

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

- Information provided as a result of the search for a CA 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 GlobalSign CA web site.
- Any other services that GlobalSign CA might advertise or provide through its web site.

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

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

10.6.4.1 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign 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 CA certificate. The GlobalSign CA takes all steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the GlobalSign Repositories and web site may result in terminating the relationship between the GlobalSign CA and the party.

10.6.4.2 Accuracy of Information

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

10.6.5 GlobalSign CA Obligations

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

- Comply with this CP and its amendments as published under http://www.globalsign.com/repository
- Provide infrastructure and certification services, including the establishment and operation of the GlobalSign CA Repository and web site for the operation of public certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available.

- Issue electronic certificates in accordance with this CP and fulfil its obligations presented herein.
- Revoke certificates issued according to this CP upon receipt of a valid and authenticated request to revoke a certificate from an RA.
- Publish accepted certificates in accordance with this CP.
- Provide support to subscribers and relying parties as described in this CP.
- Provide for the expiration and renewal of certificates according to this CP.
- Publish CRLs and/or OCSP responses of all 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 GlobalSign CA repository.

The liability of GlobalSign CA under the above stated article for proven damages is limited to 1 Euro for any individual certificate, directly caused by the occurrences listed above. This limit might be reviewed by GlobalSign. GlobalSign might seek additional insurance coverage against risks emanating from the correctness of the information included in a certificate. GlobalSign makes available a limited warranty policy.

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

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

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

10.6.6 Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign 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 GlobalSign CA.
- Ensure that the public key submitted to GlobalSign 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 GlobalSign CA.
- Receive applications for the GlobalSign CA certificates in accordance with this GlobalSign CP.
- Carry out all verification and authenticity actions prescribed by the GlobalSign CA procedures and this CP.
- Submit to the GlobalSign CA the applicant's request in a signed message (certificate request).

- Receive, verify and relay to the GlobalSign CA all requests for revocation of a GlobalSign CA certificate in accordance with the GlobalSign CA procedures and the GlobalSign 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.

10.6.7 Information incorporated by reference into a digital certificate

The GlobalSign 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 GlobalSign 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.

10.6.8 Pointers to incorporate by reference

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

10.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

10.7.1 Limitation for Other Warranties

The GlobalSign CA does not warrant:

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

10.7.2 Exclusion of Certain Elements of Damages

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

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

10.8 Limitations of Liability

The total liability of the GlobalSign is limited in accordance with the Limited Warranty Policy of GlobalSign.

Further information on the warranty conditions can be found at: http://www.globalsign.com/repository

10.9 Indemnities

This section contains the applicable indemnities.

10.9.1 Indemnity

To the extent permitted by law the subscriber agrees to indemnify and hold the GlobalSign 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 GlobalSign 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
- Attend to the integrity of the GlobalSign Root.

10.10 Term and Termination

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

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

10.11 Individual notices and communications with participants

The GlobalSign 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 GlobalSign 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 GlobalSign CA must be addressed to: legal@globalsign.com or by post to the GlobalSign in the address mentioned in the introduction of this document.

10.12 Amendments

Changes to this CP are indicated by appropriate numbering.

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

10.13 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 GlobalSign of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, GlobalSign convenes a Dispute Committee that advises GlobalSign 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 GlobalSign 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 GlobalSign executive

management. The GlobalSign executive management may subsequently communicate the proposed settlement to the resting party.

10.13.1 Arbitration

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CP, 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 CP 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.

10.14 Governing Law

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

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

10.15 Compliance with Applicable Law

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

10.16 Miscellaneous Provisions

10.16.1 Survival

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

10.16.2 Severability

If any provision of this CP, 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. .

11. List of definitions

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

DIGITAL SIGNATURE

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

DISTINGUISHED NAME

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

DIRECTORY SERVICE

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

END-USER SUBSCRIBER

A subscriber other than another CA.

ENHANCED NAMING

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

EXTENSIONS

Extension fields in X.509 v.3.0 certificates.

GENERATE A KEY PAIR

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

HASH

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

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

IDENTIFICATION

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

INCORPORATE BY REFERENCE

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

KEY GENERATION PROCESS

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

KEY PAIR

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

NOTICE

The result of notification to parties involved in receiving CA services in accordance with this CP.

NOTIFY

To communicate specific information to another person as required by this CP and applicable law.

NOTARISED TIME STAMPING

Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis with up-to-date technology.

OBJECT IDENTIFIER

A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

PKI HIERARCHY

A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.

PRIVATE KEY

A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.

PUBLIC KEY

A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

PUBLIC KEY CRYPTOGRAPHY

Cryptography that uses a key pair of mathematically related cryptographic keys.

PUBLIC KEY INFRASTRUCTURE (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.
REGISTRATION AUTHORITY OR **RA**:
An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.
RELATIVE DISTINGUISHED NAME (RDN)
A set of attributes that distinguishes the entity from others of the same type.
RELIANCE
To accept a digital signature and act in a way that shows trust in it.
RELYING PARTY
Any entity that relies on a certificate for carrying out any action.
REPOSITORY
A database and/or directory listing digital certificates and other relevant information accessible on-line.
REVOKE A CERTIFICATE
To permanently end the operational period of a certificate from a specified time forward.
SECRET SHARE
A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.
SECRET SHARE HOLDER
An person that holds a secret share.
SHORT MESSAGE SERVICE (SMS)
A service for sending messages 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.
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.
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, or revocation of certificates, including operations that restrict access to a repository.
TPM
Trusted Platform Module – A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM .
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.
GLOBALSIGN CA REGISTRATION AUTHORITY:
An entity that verifies and provides all subscriber data to the GlobalSign CA.
GLOBALSIGN CA PUBLIC CERTIFICATION SERVICES
A digital certification system made available by GlobalSign CA as well as the entities that belong to the GlobalSign CA domain as described in this CP.
GLOBALSIGN CA PROCEDURES
A document describing the GlobalSign CA's internal procedures with regard to registration of end users, security etc.
WEB -- WORLD WIDE WEB (WWW)
A graphics based medium for the document publication and retrieval of information on the Internet.
WRITING
Information accessible and usable for reference.
X.509
The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

12. 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
GSCA: GlobalSign 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