GlobalSign
Certificate Policy

Date: 15th March 2013

Version: v.4.4

Table of Contents

Document History

Version	Release Date	Author	Status + Description

V2.0	30.06.05	Andreas Mitrakas	Second version
V2.2	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
V3.5	17.05.10	Steve Roylance	Added TrustedRoot audit requirements
V4.0	22.03.12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CABForum Minimum Guidelines for issuance of SSL certificates.
V4.1	29.03.12	Lila Kee	Addition of support for NAESB.
V4.2	07.06.12	Steve Roylance	Additional CABForum Guideline support
V4.3	01.07.12	Steve Roylance	Additional CABForum Requirements
V4.4	15.03.13	Giichi Ishii Lila Kee	Extended validity period of Personal Sign, Administratie updates. Modification to NAESB certificates incorporating WEQ-012 v 3.0 updates

Acknowledgments

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

- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.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
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- X509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- North American Energy Standards Board (NAESB)Public Key Infrastructure (PKI) Standards – WEQ-012 V3.0

This CP is assessed according to the requirements of the following schemes and endorses these in whole or in part:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities.
- AICPA/CICA, WebTrust For Certification Authorities – Extended Validation Audit Criteria.
- CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

1.0 Introduction

This Certificate Policy (CP) applies to the products and services of GlobalSign nv/sa. Primarily this pertains to the issuance and lifecycle management of Digital Certificates including validity checking services. GlobalSign nv/sa may also provide additional services such as time-stamping. This CP may be updated from time to time as outlined in section 1.5 *Policy Administration*. The latest version may be found on the GlobalSign Group Company repository https://www.globalsign.com/repository. (*Alternative languages versions may be available to aid relying parties and subscribers in their understanding, however, this version remains the primary source).*

A CP is a *"named set of rules that indicates the applicability of a Digital Certificate to a particular community and/or class of application with common security requirements"*. This CP 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 to Services of GlobalSign nv/sa. These sections have *'No stipulation'* appended. Where necessary additional information is presented in subsections to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides relying parties with advance notice on the practices and procedures. Additional assertions on standards used in this CP can be found under section *"Acknowledgements"* on the previous page.

This CP addresses areas of policy & practice such as, but not limited to, Technical Requirements, Security Procedures, Personnel & Training needs, which are required to meet industry best practice for Certificate Lifecycle Management. This CP applies to all certificates issued by GlobalSign nv/sa including its Root Certificates and any chaining services to third party Sub/Issuer CAs. Root Certificates are used to manage certificate hierarchies through the creation of one or more Sub CAs that may or may not be controlled directly by the same entity that manages the Root itself.

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 CA") and the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by the Certification Authority referring to this CP.

For Subscribers this CP becomes effective and binding by accepting a Subscriber Agreement or Terms of use Agreement. For Relying Parties this CP becomes binding by relying upon a certificate issued under this CP. In addition, Subscribers are bound by the Subscriber Agreement to inform their Relying Parties that the CP is itself binding toward those relying parties.

1.1 Overview

This CP applies to the complete GlobalSign Hierarchy of GlobalSign CA and all certificates that it issues either directly through its own systems or indirectly through its TrustedRoot™ *(Previously known as Root Sign)* program including self signed Root Certificates and Keys. The purpose of this CP is to present GlobalSign CAs practices and procedures in managing Root Certificates and Issuing CAs in order to demonstrate compliance with formal industry accepted accreditations such as WebTrust and WebTrust 2.0. Additionally the Belgian Law of 9 July 2001 implementing the European Directive 1999/93/EC of the Council and the Parliament on a Community Framework on Electronic Signatures provides for the recognition of electronic signatures that are used for the purposes of authentication or non repudiation. In this regard GlobalSign CA operates within the scope of the applicable sections of the Law when delivering its services.

This CP sets out the objectives, roles, responsibilities and practices of all entities involved in the lifecycle of certificates issued under this. In simple terms a CP states *"what is to be adhered to"*, setting out an operational rule framework for products and services.

A Certification Practice Statement (CPS) complements this CP and states, *"how the Certification Authority adheres to the Certificate Policy"*. A CPS provides an end user with a summary of the processes, procedures and overall prevailing conditions that the Issuer CA *(i.e. the entity which provides the subscriber its certificate)* will use in creating and maintaining such certificates. GlobalSign CA itself maintains several CPS where certificates are delivered under alternative brands, however the CP remains consistent. Likewise GlobalSign CA TrustedRoot Subscribers who themselves become an *Issuer CA* maintain their own Certificate Practice Statement applicable to products and services they offer.

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

- Business Continuity and Disaster Recovery
- Security Policy
- Personnel Policies
- Key management Policies
- Registration Procedures

Additionally, other pertinent documents include:

- The GlobalSign Limited Warranty Policy that addresses issues on insurance.
- The GlobalSign Privacy Policy on the protection of personal data.
- The GlobalSign Certification practice Statement that addresses the methods and rules by which certificates are delivered for the domain of the GlobalSign top roots.

All applicable GlobalSign CA policies have been subjected to continuous audit and scrutiny of authorised third parties which GlobalSign CA highlights on its public facing web site via a WebTrust site seal. Additional information can be made available upon request.

The exact names of the GlobalSign CA certificates that make use of this CP are:-

- GlobalSign Root CA – R1 with serial number 040000000001154b5ac394
- GlobalSign Root CA – R2 with serial number 0400000000010f8626e60d
- GlobalSign Root CA – R3 with serial number 040000000000121585308a2
- GlobalSign Root CA – R4 with serial number 2a38a41c960a04de42b228a50be8349802
- GlobalSign Root CA – R5 with serial number 605949e0262ebb55f90a778a71f94ad86c

GlobalSign CA actively promotes the inclusion of these Roots into hardware and software platforms that are capable of supporting digital certificates and associated cryptographic services. Where possible, GlobalSign CA will seek to enter into a contractual agreement with platform providers to ensure effective Root certificate lifecycle management. However, GlobalSign CA also actively encourages platform providers at their own discretion to include GlobalSign CA Root certificates without contractual obligation.

TrustedRoot is a GlobalSign CA service, which allows third-party Issuer CAs to chain to one of the GlobalSign CA certificates.

- GlobalSign Trusted Platform Module Root CA with s/n 040000000000120190919AE [2]

TrustedRoot TPM is the GlobalSign service which allows third-party Issuing CAs to chain to the GlobalSign Trusted Platform Module Root CA certificate.

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, A Certification Authority provides confirmation of the relationship between a named entity (subject) and its public key. For TrustedRoot CA's, the purpose of entering the GlobalSign hierarchy is to enhance trust in a Issuer CA's own hierarchy, as well as providing greater functionality within third party applications such as web browsers. This endeavour does not undermine the ability of GlobalSign to revise its approach and seek alternative strategies in the future. It is the duty of any TrustedRoot Issuer CA to assess the value of the GlobalSign services at any point in time and act accordingly.

[2] *Collectively Root R1 to R5 and the TPM Root are referred to as the GlobalSign CA Root Certificates*

The process to obtain a digital certificate includes the identification, naming, authentication and registration of an applicant as well as aspects of certificate management such as the issuance, revocation and expiration. By means of this policy, GlobalSign CA provides adequate and positive confirmation about the identity of the subject of a certificate and a positive link to the public key that such an entity uses. An entity in this instance might include an end user or another certification authority. GlobalSign CA makes available digital certificates that can be used for non-repudiation, encryption and authentication. The use of these certificates can be further limited to a specific business or contractual context with transaction levels recommended by the associated warranty policy.

GlobalSign CA accepts comments regarding this CP addressed to the address mentioned in section 1.5. *(Policy Administration)*

1.1.1 Additional requirements for TrustedRoot Issuer CAs

This CP also addresses the TrustedRoot program for appropriately authorized Issuer CAs. Entering the GlobalSign CA hierarchy is carried out through a CA chaining program that GlobalSign CA makes available to interested parties under the TrustedRoot brand. TrustedRoot CA certificates are usually:-

- Issued by GlobalSign CA to a third party Issuing CA that meets the contractual, audit and policy requirements of GlobalSign CA TrustedRoot services with regard to operational practices and technical implementation.
- Issued only to Enterprise in-house CA's to issue SSL and/or S/MIME certificates for use under their own brand towards their own target audience.
- Provide allowance for additional Certificate types as required to provide lifecycle management such as but not limited to key escrow certificates and OCSP signing certificates.
- Not allowed to be used for code-signing certificates.
- Constrained to specific domains for either/or SSL & S/MIME usage to protect both the third party and GlobalSign Hierarchy.

GlobalSign CA actively forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection and therefore seeks to maintain a position of leadership with regard to inclusion of its Roots in third party applications.

1.2 Document Name and Identification

This document is the GlobalSign CA Certificate Policy.

The OID for GlobalSign nv/sa is a iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign nv-sa (4146). GlobalSign organizes its OID arcs for the various certificates and documents described in this CP as follows:

1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy – SSL
1.3.6.1.4.1.4146.1.2	Extended Validation Certificates Policy – Code Signing
1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy
1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificates Policy - AlphaSSL
1.3.6.1.4.1.4146.1.10.20	~~Domain Validation Certificates Policy – SignTrust~~ *(DEPRECATED)*
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
1.3.6.1.4.1.4146.1.40.10	Client Certificates Policy (ePKI – Enterprise PKI)
1.3.6.1.4.1.4146.1.40.20	Client Certificates Policy (JCAN – Japan CA Network)
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 – TrustedRoot™
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
2.16.840.1.114505.1.12.1.2	NAESB Rudimentary Assurance
2.16.840.1.114505.1.12.2.2	NAESB Basic Assurance
2.16.840.1.114505.1.12.3.2	NAESB Medium Assurance
2.16.840.1.114505.1.12.4.2	NAESB High Assurance

In addition to these identifiers, all certificates that comply with the CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates will include the additional identifiers as follows:-

2.23.140.1.2.1	Domain Validation Certificates Policy
2.23.140.1.2.2	Organization Validation Certificates Policy

1.3 PKI participants

1.3.1 Certification Authorities ("Issuer CAs")

A Certification Authority (CA)'s primary responsibility is to perform functions related to PKI (Public Key Infrastructure) functions such as certificate lifecycle management, subscriber registration, certificate issuance, certificate renewal, certificate distribution and certificate revocation. Certificate status information may be provided using an online repository in the form of a CRL (Certificate Revocation List) distribution point and/or OCSP (Online Certificate Status Protocol) responder. A Certification Authority may also be described by the term *"Issuing Authority or Issuer CA"* to denote its purpose of issuing certificates at the request of an RA (Registration Authority) from a subordinate Issuer CA which may or may not be managed by GlobalSign CA. (i.e. A TrustedRoot issuer CA)

The GlobalSign CA Policy Authority, which is composed of members of the GlobalSign management team and appointed by it's Board of Directors, is responsible for maintaining this Certificate Policy relating to all digital certificates in the GlobalSign hierarchy. Through its Policy Authority GlobalSign CA has ultimate control over the lifecycle and management of the GlobalSign Root and any subsequent Sub CA including TrustedRoot Issuer CAs belonging to the hierarchy.

GlobalSign CA operates a secure facility in order to deliver CA services through an outsource agent. The GlobalSign CA outsource agent operates a service to GlobalSign CA on the basis of a service agreement. The scope is certificate issuance and revocation services. The GlobalSign CA outsources agent warrants designated services and service levels that meet those required by GlobalSign CA. The GlobalSign CA outsource agent carries out tasks associated with the administration of services and certificates on behalf of GlobalSign CA. GlobalSign CA outsource agents are located in Belgium and France.

Henceforth and for ease of reference all CAs issuing certificates in accordance with this CP (including GlobalSign CA) shall be referred to as Issuer CAs.

Issuer CAs ensures the availability of all services relating to the management of certificates issued. Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of revoked certificates. Issuer CAs provides Certificate status information using an online repository in the form of a CRL (Certificate Revocation List) distribution point and/or OCSP (Online Certificate Status Protocol) responder as indicated within the digital certificate properties.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that identifies and authenticates applicants for certificates. A RA may also initiate or pass along revocation requests for certificates and requests for re-issuance and renewal (sometimes referred to as rekey) of certificates. Issuer CAs may act as a Registration Authority for certificates it issues in which case they are responsible for:

- Accepting, evaluating, approving or rejecting the registration of certificate applications.
- Registering subscribers for certification services.
- Providing systems to facilitate the identification of subscribers (according to the type of certificate requested).
- Using officially notarised or otherwise authorised documents or sources of information to evaluate and authenticate a subscriber's application.
- Following approval of an application requesting issuance of a certificate via a multifactor authentication process.
- Initiating the process to revoke a certificate from the applicable GlobalSign subordinate issuing CA.

Third party Issuing CAs, who enter into a contractual relationship with GlobalSign CA may operate their own RA and authorize the issuance of certificates. Third parties must abide by all the requirements of this CP and the terms of their contract which may also refer to additional criteria as recommended by the CABForum. RA's may implement more restrictive vetting practices if their internal policy dictates.

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

RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of RAs or as in the case of ePKI (Enterprise PKI) and MSSL (Managed SSL) are constrained by pre defined and validated GCC (GlobalSign Certificate Centre) configurations. These entities also commonly known as Enterprise RAs

1.3.3 Subscribers

Subscribers of Issuing CAs are either directly reliant on the Issuing CA to issue end entity certificates from a hierarchy managed by the Issuing CA or they are third parties that seek to be issued with an Issuing CA capable of issuing additional certificates to their own PKI hierarchy. Subscribers are either legal persons or individuals that successfully apply for and receive a certificate to support their use in transactions, communications and the application of digital signatures. In some cases individuals are not able to obtain certain certificate types.
The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the Issuing CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

End Entity Subscribers:

- Have ultimate authority over the private key corresponding to the public key that is listed in a subscriber's certificate. A subscriber may or may not be the Subject of a certificate (For example machine or role based certificates issued to firewalls, routers, servers or other devices used within an Organization)

Trusted Root Subscribers:

- Set the framework of providing certification services with the CA hierarchy for the benefit of the subject mentioned in a certificate.
- Accept and implement the contractual, audit and policy requirements of GlobalSign TrustedRoot services with regard to operational practices and technical implementation.
- Can only be Enterprise in-house PKI's. No public PKI services are allowed.
- GlobalSign reserves the right to technically constrain the breadth of a domain through the use of subordination (For example RFC 5280 dNSName Name Constraints)

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

- **PersonalSign 2**
- **GlobalSign CA for AATL**
- **Code Signing**

Natural or Department / role-based legal persons within an Organizational context can be listed as Subjects of the following certificates:

- **PersonalSign 2 Pro**
- **PersonalSign 3 Pro**
- **NAESB v3.0**
- **GlobalSign CA for AATL**

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

- **ExtendedSSL**
- **GlobalSign Timestamping**
- **Extended Validation Code Signing**

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

- **OrganizationSSL**
- **Code Signing**

DNS Names may be listed as the subject of the following certificates.

- **DomainSSL**
- **AlphaSSL**

RFC822 e-mail addresses may be listed as the subject of the following certificates.

- **PersonalSign 1/PersonalSign Demo**

1.3.4 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, business partners of a Trusted Root partner that receive S/MIME certificates issued by the TrustedRoot Subscriber's CA are effectively subscribers and relying parties at the same time.

To verify the validity of a digital certificate, relying parties must always refer to Issuing CA revocation information which is usually presented in the applicable end entity certificate and appropriate chain of certificates.

1.3.5 Other Participants

Other participants include Bridge CAs and CAs that cross certify Issuing CAs to provide trust among other PKI communities.

1.4 Certificate usage

A digital certificate is a specifically formatted data object that cryptographically binds an identified subscriber with a Public Key (supporting either RSA or ECC). A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage.

Subordinate CA certificates issued under the GlobalSign TrustedRoot Program can be used to issue digital certificates for transactions that require:

- Authentication
- Assurance about the identity of a remote device
- Encryption

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

1.4.2 Prohibited certificate usage

Certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorised. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the Limited Warranty Policy.

Certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the certificate has been installed is not free from defect, malware or virus. In the case of Code Signing, certificates do not guarantee that signed code is free from bugs or vulnerabilities.

Certificates issued under this CP may not be used:-

- for any application requiring fail safe performance such as
  - the operation of nuclear power facilities,
  - air traffic control systems,
  - aircraft navigation systems,
  - weapons control systems,
  - any other system whose failure could lead to injury, death or environmental damage;
- where prohibited by law.
- Certificates issued under the NAESB WEQ PKI shall never be used for performing any of the following functions:
  - Any transaction or data transfer that may result in imprisonment if compromised or falsified.
  - Any transaction or data transfer deemed illegal under federal law

1.4.2.1 Certificate extensions

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.

Issuing CAs use 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 capability of a CA or subscriber certificate so that such subscribers can be identified under varying roles.

Key usage extensions limit the technical purposes for which a public key listed in a certificate may be used. Issuing CA certificates may contain a key usage extension that limits the functionality of a key to only signing certificates, certificate revocation lists or the subjects from a specific domain.

A certificate policy extension limits the usage of a certificate to the requirements of a business or a legal context. Issuing CAs should pro-actively support and participate in the proliferation of industry, government or other certificate policies for their public certificates as they deem appropriate.

1.4.2.2 Critical Extensions

Issuing CA 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 as a CA or not.
- To show the intended usage of the key.
- To show the number of levels in the hierarchy under a CA certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

GlobalSign NV
Principle 1 Policy Authority
GlobalSign NV
Martelarenlaan 38
3010 Leuven,
Belgium.
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909

1.5.2 Contact Person

GlobalSign NV
attn. Legal Practices,
Martelarenlaan 38
3010 Leuven,
Belgium.
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

1.5.3 Person Determining CP Suitability for the Policy

The Principle 1 Policy Authority determines the suitability and applicability of this CP and the conformance of a CPS to this CP based on the results and recommendations received from an independent WebTrust auditor. Each Policy Authority, as described below, is responsible for evaluating and acting upon the results of compliance audits.

In an effort to invoke credibility and Trust in this CP and to better correspond to accreditation and legal requirements, the Policy Authority may make revisions and updates to policies as it sees fit or as required by other 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 this CP.

New versions and publicized updates of appropriate policies are approved by one of three Policy Authorities which relate to either, Public Practices *(WebTrust Principle 1 Policy Authority),* Vetting Practices *(WebTrust Principle 2 Policy Authority)* or Security Practices *(WebTrust Principle 3 Policy Authority).* Each Policy Authority in its present organisational structure comprises members as indicated below:

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

The Management member chairs the applicable Policy Authority ex officio and each Policy Authority reports to the Board of Directors of GlobalSign nv/sa.

All members of each Policy Authority have one vote to determine the suitability of the Policy. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chair of the Policy Authority counts double.

Each Policy Authority chair is also responsible for implementation of any independent third party auditor feedback into applicable polices.

1.5.4 CP Approval Procedures

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

The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CP is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the 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 (Webtrust Auditor) may submit objections to policy changes. Relying parties that are not subscribers do not have the right to submit objections.

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

1.5.4.1 Changes with notification

Updated versions of this CP are submitted to Issuing CA Auditors and the three Policy Authorities.

1.5.4.2 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

1.6 Definitions and acronyms

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate Request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct.

Audit Criteria: The requirements described in this document and any requirements that an entity must follow in order to satisfy the audit scheme selected under section 16.1

Audit Report: A statement, report, or letter issued by a Qualified Auditor stating a CA's or RA's compliance with these Requirements.

Binding: A statement by an RA of the relationship between a named entity and its public key.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Request: Communications described in Section 10 requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

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.

Domain Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Effective Date: The date, as determined by the eligible audit schemes, on which Requirements come into force.

Enterprise Certificate: A Certificate whose issuance is authorized by an Enterprise RA.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

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

Hash: (e.g. SHA1 or SHA256) - 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.

HSM: Hardware Security Module: A HSM is type of secure cryptoprocessor targeted at managing digital keys, accelerating cryptoprocesses in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

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.

Independent Audit: An audit that is performed by a Qualified Auditor and that determines an entity's compliance with these Requirements and one or more of the audit schemes listed in Section 16.1.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) Standards WEQ-012 v3.0: The technical and management details which a certification authority is required to meet in order to be accredited as an Authorized Certification Authority (ACA) by NAESB

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of certificates, but is not a CA, and hence does not sign or issue certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures for the generation of the Root CA Key Pair**.**

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.

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 are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

AICPA	American Institute of Certified Public Accountants
ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
ETSI	European Telecommunications Standards Institute
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GSCA	GlobalSign Certification Authority
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IM	Instant Messaging
ISO	International Organization for Standardization
ISO	International Standards organization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NAESB	North American Energy Standards Board
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol

OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax
VOIP	Voice Over Internet Protocol

2.0 Publication and Repository Responsibilities

2.1 Repositories

The Issuer CA shall publish all CA certificates and cross - certificates issued to and from the Issuer CA, revocation data for issued certificates, CP, CPS, and Relying Party Agreements and Subscriber Agreements in online repositories. The Issuer CA shall ensure that revocation data for issued certificates and its root CA are available through a repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down - time that does not exceed 0.5% annually

All parties who are associated with the issuance, use or management of Issuer CA certificates are hereby notified that Issuer CAs may publish submitted information on publicly accessible directories for the provision of certificate status information.

Issuer CAs may refrain from making publicly available certain elements of documentation including security controls, procedures, internal security polices etc. However elements may be disclosed in audits associated with formal accreditation schemes that GlobalSign adheres to, such as WebTrust for CAs and WebTrust for EV.

Country specific web sites and translations of this CP and other public documentation may be made available by Issuing CAs for marketing purposes however the legal repository for all GlobalSign CA Public facing documentation is https://www.globalsign.com/repository and the in the event of a dispute the English version shall be deemed the master.

2.2 Publication of Certificate Information

Issuer CAs shall make publically available this CP and any CPS, CA certificates, Subscriber Agreements, Relying Party Agreements, and CRLs in online repositories. CRLs should contain entries for all revoked unexpired certificates. Issuer CAs may choose to maintain the serial numbers of expired certificates on a CRL to further promote additional security assertions.

2.3 Time or Frequency of Publication

CA certificates are published in a repository via support pages as soon as possible after issuance. CRLs for end - user certificates are issued at least every 3 hours. CRLs for CA certificates are issued at least every 6 months and within 24 hours if a CA certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

New or modified versions of this CP, the CPS, Subscriber Agreements, or Relying Party Warranties are published within seven days after being digitally signed by the CPS (Principle 1 Policy Authority) using an Adobe CDS PDF signing certificate with appropriate time stamp.

2.4 Access control on repositories

The Issuer CA shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories. In the case of GlobalSign CA, the integrity and authenticity of its public documentation is maintained through the use of digital signatures applied to PDF documents.

3.0 Identification and Authentication

Issuers CAs maintain documented practices and procedures to authenticate the identity and/or other attributes of the certificate applicant.

Issuer CAs use approved procedures and criteria to accept applications from entities seeking to become part of the CAs hierarchy, either as Sub CA seeking chaining services or as an RA, Enterprise RA or as an end entity subscriber.

Issuer CAs must authenticate the requests of parties wishing to perform revocation of certificates under this policy.

3.1 Naming

3.1.1 Types of Names

To identify a subscriber Issuer CAs shall follow 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. Where DNs (Distinguished Names) are used, CNs (Common Names) must respect name space uniqueness and must not be misleading. RFC2460 (IP version 6) or RFC791 (IP version 4) addresses may be used.

3.1.2 Need for Names to be Meaningful

When applicable, Issuer CAs shall use distinguished names to identify both the subject and issuer of the certificate. When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

3.1.3 Anonymity or Pseudonymity of Subscribers

Issuer CAs may issue end - entity anonymous or pseudonymous certificates provided that such certificates are not prohibited by applicable policy and that name space uniqueness is preserved.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

Issuer CAs may enforce uniqueness within the DN or by requiring that each certificate include a unique non-sequential serial number with at least 20 bits of entropy.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with any content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated, this CP does not require that an Applicant's right to use a trademark be verified. However, Issuer CAs may reject any applications or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

Issuer CAs may perform identification of the applicant for a certificate or for services including CA chaining services using any legal means of communication or investigation necessary to identify the legal person or individual.

Issuer CAs may use the result of a successful Subject DN Initial Identity Validation process to create alternative product offerings by effectively combining elements of previously verified information with alternative, newly verified, information. A suitable Account based challenge response mechanism must be used to authenticate any previously verified information for any returning Applicant noting that the aging requirements of section 3.3.1 must be upheld.

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the private key corresponding to the public key being registered with the Issuing CA. Such a relationship can be proved by, for example, a digital signature in the CSR (Certificate Signing Request) in addition to an out-of-band confirmation.

Issuer CAs may accept other Issuer CAs wishing to enter their hierarchy though the TrustedRoot Program. Following an initial assessment and signing of a specific agreement with the Issuer CA the applicant sub CA must also prove possession of the private key. CA chaining services do not mandate the physical appearance of the subscriber representing the sub CA so long as an agreement between the applicant organisation (which has been authenticated) and the Issuer CA has been executed.

3.2.2 Authentication of Organization Identity

For all certificates that include an Organization Identity, Applicants are required to indicate the Organization's name and registered or trading address. The Legal existence, Legal name, Legal form and provided address of the Organization must be verified either through a Registration Body in the Jurisdiction of Incorporation/Formation of the Organization or an alternative suitable Qualified Government Information Source (QGIS). A Qualified Independent Information Source (QIIS) may also be used to replace or augment the QGIS so long as an Issuer CA clearly states this within its CPS. Alternatively, a Legal Opinion providing additional confirmation of any of the facts required to authenticate the Organization's Identity may be sought.

The authority of the Applicant to request a certificate on behalf of the Organization must be verified in accordance with section 3.2.5.

For SSL/TLS Certificates, the applicant's ownership or control of all requested Domain(s) must be verified by a suitable method such as the inspection of WHOIS records, contact with the Domain Registrar, email challenge/responses in line with CABForum Base Requirements or an alternative practical demonstration of control of the Domain(s).

Further information may be requested from the Applicant and other information and or methods may be utilized in order to achieve an equivalent level of confidence.

3.2.2.1 Local Registration Authority Authentication

For accounts that allow the concept of a Local Registration Authority, Issuer CAs and RAs may fix authenticated Organizational details in the form of a *Profile.* Suitably authenticated Account Administrators acting in the capacity of a Local Registration Authority must authenticate individuals affiliated to the Organization and/or any sub-domains owned or controlled by the Organization. (Whilst LRA's are able to authenticate individuals under contract, all domains to be authenticated must have previously had the appropriate higher-level domain pre-authorized and authenticated in line with this CP and with CABForum Minimum Guidelines).

3.2.2.2 Role Based Certificate Authentication (DepartmentSign)

Issuer CAs must ensure that requests for Role Based Certificates are authenticated either by a RA, acting on behalf of the CA, or a LRA that is contractually obligated to the Issuer CA/RA to ensure that Role Based names relating to the Organization and its business are accurate and correct.

Role based Certificates must not be made available to individuals.

3.2.2.3 Extended Validation Certificates (SSL and Code Signing)

For Extended Validation Certificates, the CAB Forum EV guidelines must be followed.

3.2.3 Authentication of Individual identity

Issuer CAs or RAs shall Authenticate Individuals depending upon the class of certificate as indicated below.

3.2.3.1 Class 1 (PersonalSign 1 & PersonalSign 1 Demo Certificates)

The Applicant is required to demonstrate control of the email address to which the certificate relates. Issuer CAs or RAs are not required to authenticate any other information provided.

3.2.3.2 Class 2 (PersonalSign2, SSL, CodeSigning & AATL for Individuals)

The Applicant is required to demonstrate control of any email address to be included within a certificate.

The Applicant is required to submit a legible copy of a valid government issued National Identity Document or Photo ID (Drivers Licence, Military ID or equivalent). A suitable non-government issued Identity Document or Photo ID may also be required for additional proof. Issuer CAs are required to verify to a reasonable level of assurance that the copy of the ID matches the requested name and that other subject information such as Country and/or State and Locality fields are authenticated.

Issuer CAs or RAs are also required to authenticate the Applicant's identity through one of the following methods;

- Performing a telephone challenge/response to the Applicant using a number from a reliable source, or;
- Performing a postal challenge to the Applicant using an address obtained from a reliable source, or;

- Receiving an attestation from an appropriate Notary, Trusted Third Party that they have met the individual, and have inspected their National Photo ID document, and that the application details for the order are correct, or;
- The applicant's Seal Impression, (In jurisdictions that permit their use to legally sign a document) is included with any application received in writing.

Further information may be requested from the Applicant. Other information and/or methods may be utilized in order to demonstrate an equivalent level of confidence.

3.2.3.3 Class 3 (PersonalSign3 Pro Certificates)

The Applicant is required to demonstrate control of any email address to be included within a certificate.

The Applicant is required to submit a legible copy of a valid government issued National Identity Document or Photo ID (Drivers Licence, Military ID or equivalent). A suitable non-government issued Identity Document or Photo ID may also be required for additional proof. Issuer CAs are required to verify to a reasonable level of assurance that the copy of the ID matches the requested name and that other subject information such as Country and/or State and Locality fields are authenticated.

A face to face meeting is required to establish the Individual's identity with an attestation from the Notary or Trusted Third Party that they have met the individual and have inspected their National Photo ID document, and that the application details for the order are correct.

The issuing CA is also required to authenticate the applicant's authority to be bound to the Organizational subject by one of the following methods;

- Performing a telephone challenge/response to the Applicant's Organization using a number from a reliable source, or;
- Performing a postal challenge to the Applicant's Organization using an address obtained from a reliable source, or;

Further information may be requested from the Applicant or the Applicant's Organization. Other information and/or methods may be utilized in order to achieve an equivalent level of confidence.

3.2.3.4 Local Registration Authority Authentication

For accounts that allow the concept of a Local Registration Authority, Issuer CAs and RAs may fix authenticated Organizational details in the form of a *Profile.* Suitably authenticated Account Administrators acting in the capacity of a Local Registration Authority must authenticate individuals affiliated to the Organization.

3.2.3.5 North American Energy Standards Board (NAESB) Certificates

For NAESB certificate requests, Authenticity of Organization Identity Requests for Subscriber Certificates in the name of an affiliated organization shall include the organization name, address, and documentation of the existence of the organization. GlobalSign or RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization. End Entities shall be obligated to register their legal business identification and secure an "Entity Code" that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that End Entity.

GlobalSign may elect to perform RA Operations/Functions in-house or choose to delegate some, or all, RA Operations/Functions to other parties that are separate legal entities through its ePKI service. In both cases the party or parties performing RA Operations/Functions are subject to the obligations for identity proofing, auditing, logging, protection of Subscriber information, record retention and other aspects germane to the RA function outlined in this CPS and the NAESB Authorized CA Accreditation Specification. All RA infrastructure and operations performing RA Operations/Functions shall be held to this requirement as incumbent upon the Certificate Authority when performing in-house RA Operations/Functions. The Authorized Certification Authority and/or delegated entity are responsible for ensuring that all parties performing RA Operations/Functions understand and agree to conform to the NAESB Authorized CA Accreditation Specification.

For Subscribers, GlobalSign, and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by the GlobalSign CP and CPS. Process information shall depend upon the Certificate level of assurance and shall be addressed in the NAESB Authorized CA accreditation requirements. The documentation and authentication requirements shall vary depending upon the level of assurance.

Registration of Identity Proofing Requirements shall use the using the following mappings:

NIST Assurance Level	NAESB Assurance Level
Level 1	Rudimentary
Level 2	Basic
Level 3	Medium
Level 4	High

GlobalSign CA, or its designated RA in the case of ePKI, shall verify all of the following identification information supplied by the Applicant: in compliance with the authentication requirements defined by NIST SP800-63 version 1.0.2 found 1 http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

3.2.4 Non Verified Subscriber Information

Issuer CAs must validate all information to be included within the Subject DN of a certificate or clearly indicate within their CPS and within the issued Certificate itself any exceptions that may apply to specific product types or services offered. Issuer CAs may use the Subject:organizationalUnitName as a suitable location to highlight Non Verified Subscriber Information to relying parties or to highlight any specific disclaimers/notices.

- For all certificate types where the Issuer CA can explicitly identify a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity the Issuer CA must verify the information and may therefore omit a disclaimer notice.

- For all certificate types where the Issuer CA cannot explicitly verify the identity e.g. a generic term such as "Marketing" then the Issuer CA may also omit the disclaimer noting that this item is therefore classified as Non Verified Subscriber Information. For OV SSL/TLS certificates only, Issuer CAs may rely upon information provided by the applicant to be included within the subjectAlternativeName such as internal or non public-DNS names, hostnames and RFC 1918 IP addresses. CABForum Base Requirement guidelines define the timelines for which these types of objects may be included within certificates and again these items may be classified as Non Verified Subscriber Information.

Specifically for SSL/TLS certificates and Code Signing Certificates, the CA must maintain a process to ensure that Applicants cannot add self reported information to the subject:organizationalUnitName.

Issuing CAs that provide client authentication, document signing, secure messaging and role based certificates may contractually allow Local Registration Authorities to perform validation of data for the following fields so long as an Alternative Policy OID is present.

- Subject:organizationalUnitName and/or
- Common Name.

3.2.5 Validation of Authority

- **PersonalSign1 Certificates -** Verification that the applicant has control over the e-mail address to be listed within the certificate.
- **PersonalSign Demo Certificates -** Verification that the applicant has control over the e-mail address to be listed within the certificate.
- **PersonalSign2 Certificates -** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has control over the e-mail address to be listed within the certificate.
- **NAESB Certificates** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has control over the e-mail address if to be listed within the certificate as detailed in section 3.2.3.5.
- **PersonalSign3 Certificates -** Verification through a reliable means of communication with the organization that the applicant represents the organization. Personal appearance is mandatory before a suitable Registration Authority to validate the personal credentials of the applicant together with verification that the

applicant has control over the e-mail address to be listed within the certificate.

- **Code Signing Certificates –** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has control over any e-mail address that may be optionally listed within the certificate.
- **EV Code Signing Certificates –** Verifying the authority of the Contract Signer and Certificate Approver in accordance with the EV Guidelines.
- **DV/AlphaSSL Certificates –** Validation of the ownership or control of the domain name by either a challenge response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS. If a country code is to also be included within the certificate, then Issuer CAs must verify the country associated with either the Domain Name itself or the applicant making the request. Nounvetted country information may be included.
- **OV SSL Certificates –** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has ownership or control of the domain name by either a challenge response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS.
- **EV SSL Certificates –** Verifying the authority of the Contract Signer and Certificate Approver in accordance with the EV Guidelines.
- **Time Stamping Certificates –** Verification through a reliable means of communication with the organization's applicant.
- **CA for AATL Certificates –** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has control over any e-mail address to be listed within the certificate.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Re-key Requests

Issuer CAs may support rekey requests from subscribers prior to the expiry of the subscribers existing certificate. Issuer CAs may also support re-issue at any time during the lifetime of the certificate. Re-issue is a form of rekey, the primary difference being that the re-keyed certificate has a not after date which equals the not after date of the certificate that is being re-issued.

3.3.1 Identification and Authentication for Routine Re-key

- **PersonalSign1 Certificates -** Username and Password required with re-verification every 9 years.
- **PersonalSign2 Certificates -** Username and Password required with re-verification every 9 years or client authentication with a current unexpired and unrevoked certificate.
- **PersonalSign3 Certificates -** Username and Password required with re-verification every 6 years.
- **Code Signing Certificates -** Username and Password required with re-verification every 6 years.
- **EV Code Signing Certificates -** Username and Password required with re-verification as indicated by the EV guidelines.
- **DV SSL Certificates -** Username and Password required with re-verification every 5 years.
- **OV SSL Certificates -** Username and Password required with re-verification every 5 years.
- **EV SSL Certificates -** Username and Password required with re-verification as indicated by the EV guidelines.
- **Time Stamping Certificates -** Not supported
- **CA for AATL Certificates -** Username and Password required with re-verification every 6 years.
- **PDF Signing Certificates -** Not supported.
- **TrustedRoot -** Not supported.
- **AlphaSSL** Not supported

- **NAESB Certificates:** Subscribers of Authorized Certification Authorities shall identify themselves for the purpose of reissuing as required in the table below.

Assurance Level	Identity Requirements
Rudimentary	Identity may be established through use of current signature key.
Basic	Identity may be established through use of current signature key, except that identity shall be re-established through initial registration process at least once every five years from the time of initial registration.
Medium	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration.
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least annually.

Identification and Authentication for Reissuance after Revocation

After a Certificate has been revoked, the Subscriber is required to go through the initial registration process described elsewhere in this document to obtain a new Certificate.

Re-verification and Revalidation of Identity When Certificate Information Changes

If at any point any subject name information embodied in a Certificate issued by a Certificate Authority is changed in any way, the identity proofing procedures outlined in this requirement must be re-performed and a Certificate issued with the validated information.

Issuer CAs must not re - key a certificate without additional authentication if doing so would allow the Subscriber to use the certificate beyond the limits described above.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key must only be supported for certificates that have not been revoked. Revocation of a certificate mandates the subscriber to follow the initial validation process that was completed to allow the initial issuance of the certificate.

3.4 Identification and Authentication for Revocation Request

All revocation requests must be authenticated by the Issuer CA. Revocation requests from subscribers may be granted following a suitable challenge response such as, logging into an account with a suitable username and password, or proving possession of unique elements incorporated into the certificate e.g. domain name or e-mail address.
Issuer CAs may also perform revocation on behalf of subscribers in line with requirements highlighted within applicable subscriber agreements such as, but not limited to, breach of the subscriber agreement or non payment of applicable fees.

4.0 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Issuer CAs shall maintain their own blacklists for individuals from whom or entities from which they will not accept certificate applications. Blacklists may be based on past history or other sources. In addition, other external sources such as government denied lists or internationally recognised denied persons lists which are applicable to the jurisdictions in which the Issuer CA operates.

4.1.2 Enrollment Process and Responsibilities

Issuer CAs shall maintain systems and processes that sufficiently authenticate the applicants identify for all certificate types that present the identity to relying parties. Applicants should submit sufficient information to allow Issuer CAs and RAs to successfully perform the required verification. Issuer CAs and RAs shall protect all communications and securely store all information presented by the applicant during the application process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Issuer CAs shall maintain systems and processes that sufficiently authenticate the applicants identify in line with the applicable statements made in its CPS. Initial identity validation shall be performed by an Issuer CAs Validation team or by Registration Authorities under contract in line with section 3.2 of this policy. All communications shall be securely stored along with all information presented by the applicant during the application process. Future Identification of repeat applicants and subsequent authentication checks may be addressed using single or multi factor authentication principles.

4.2.2 Approval or Rejection of Certificate Applications

Issuer CAs shall reject requests for certificates where validation of all items cannot successfully be completed. Issuer CAs may also reject requests based on potential brand damage to the Issuer CA in accepting the request. Issuer CAs may also reject requests for certificates from applicants who have previously been rejected or have previously violated a stipulation within a Subscriber Agreement. Issuer CAs are under no obligation to provide a reason to an applicant on why a request has been rejected. Assuming all validation steps can be completed successfully following appropriate best practice techniques Issuer CAs shall approve the request.

4.2.3 Time to Process Certificate Applications

Issuer CAs shall ensure that all reasonable methods are used in order to process and evaluate certificate applications.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Issuer CAs shall communicate with any RA accounts capable of causing certificate issuance using multifactor authentication. RAs directly operated by the Issuer CA or RAs contracted by the Issuer CA to perform validation shall ensure that all information sent to the CA is verified and authenticated in a secure manner.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The Issuer CA shall inform the subscriber of the issuance of a certificate in a convenient and appropriate way based on information submitted during the Enrollment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Issuer CAs shall inform Subscribers that they may not use the Digital Certificate until they have reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open ended stipulation, Issuer CAs may set a time limit by when the certificate is deemed to be accepted.

4.4.2 Publication of the Certificate by the CA

Issuer CAs may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in a suitable repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

All subscribers must protect their Private Key taking care to avoid disclosure to third parties. Issuer CAs must maintain a suitable Subscriber Agreement which highlights the obligations of the subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding digital certificate. Where it is possible to make a back up of a private key, Subscribers must use the same level of care and protection attributed to the live private key. At the end of the useful life of a Key, Subscribers must securely delete the key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Issuer CAs must describe the conditions under which digital certificates may be relied upon by relying parties within their CPS including the appropriate mechanisms available to verify certificate validity (e.g. CRL or OCSP). Issuer CAs must also offer a relying party agreement to Subscribers the content of which should be presented to the relying party prior to reliance upon a digital certificate from the Issuer CA. Relying

parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the certificate or any assurances made.
Software used by relying parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is defined as the production of a new certificate that has the same details as a previously issued certificate and the same public key with the except of NAESB certificates which must rely on rekeying but contains a new 'Not After' date. Issuer CAs that support renewal must identify the products and services under which renewals can be accepted. An Issuer CA may renew a certificate so long as:-

- The original certificate to be renewed has not been revoked.
- The public key from the original certificate has not been blacklisted for any reason.
- All details within the certificate remain accurate and no new or additional validation is required.

Issuer CAs may renew certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original certificate may be revoked after renewal is complete; however, the original certificate must not be further renewed, rekeyed or modified.

4.6.2 Who May Request Renewal

An issuer CA may accept a renewal request provided that it is authorized by the original Subscriber through a suitable certificate lifecycle account challenge response. A certificate signing request is not mandatory, however if one is used then it must contain the same public key.

4.6.3 Processing Certificate Renewal Requests

An issuer CA may request additional information before processing a renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Certificate re-key is defined as the production of a new certificate that has the same details as a previously issued certificate but has a new public key and a new 'Not After' date.

If a certificate is re-keyed prior to the Not After date expiring and given the same Not After date Issuer CAs may refer to this as Re-issue.

Issuer CAs that support re-keying must identify the products and services under which re-keys can be accepted. An Issuer CA may re-key a certificate as long as:-

- The original certificate to be re-keyed has not been revoked.
- The new public key has not been blacklisted for any reason.
- All details within the certificate remain accurate and no new or additional validation is required.

Issuer CAs may re-key certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original certificate may be revoked after rekey is complete; however, the original certificate must not be further renewed, rekeyed or modified.

4.7.2 Who May Request Certification of a New Public Key

An issuer CA may accept a re-key request provided that it is authorized by either the original Subscriber, or an Organization Administrator who retains responsibility for key material on behalf of a subscriber through a

suitable certificate lifecycle account challenge response. A certificate signing request is mandatory with any new public key.

4.7.3 Processing Certificate Re-Keying Requests

An issuer CA may request additional information before processing a re-key or re-issue request and may re-validate the Subscriber subject to aging restrictions of any previously validated data. In the case of a re-issuance, authentication through a suitable challenge response mechanism is acceptable.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new certificate that has the details which differ from a previously issued certificate. The new modified certificate may or may not have a new public key and may or may not have a new 'Not After' date.

- Issuer CAs shall treat Modification in the same was a 'New' issuance.
- Issuer CAs may modify certificates that have either been previously renewed or previously rekeyed. The original certificate may be revoked after modification is complete, however, the original certificate must not be further renewed, rekeyed or modified.

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a certificate is effectively blacklisted by adding the serial number and the date of the revocation to a CRL (Certificate Revocation List). The CRL itself will then be digitally signed with the same key material which originally signed the certificate to be revoked. Adding a serial number allows relying parties to establish that the lifecycle of a digital certificate has ended. Issuer CAs may remove serial numbers once a certificate has normally expired to promote more efficient CRL file size management. Prior to performing a revocation Issuer CA's will verify the authenticity of the revocation request. Revocation may be performed under the following circumstances:-

- The Subscriber or Organization Administrator requests revocation of the Digital Certificate through a Issuer CA provided account which controls the lifecycle of the Digital Certificate,

- The Subscriber requests revocation through an authenticated request to Issuer CA's Support team or Registration Authority,
- Issuer CAs obtain reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised, created using a weak algorithm, or that the Digital Certificate has otherwise been misused,
- Issuer CAs receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement,
- Issuer CAs receive notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, certifying or signing malware etc.,
- Issuer CAs receive notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use any of the elements within the 'Subject' or 'Subject Alternative Name' of the Digital Certificate, or that the Subscriber has failed to renew or maintain control of any of those elements,
- Issuer CAs receive notice or otherwise becomes aware of a material change in the information contained in the Digital Certificate,
- A determination, under the Issuer CAs sole discretion, that the Digital Certificate was not issued according to best practice or any of the Issuer CAs own published policies,
- If Issuer CAs determine that any of the information appearing in the Digital Certificate is not accurate,
- Issuer CAs cease operations for any reason and have not arranged for another Issuer CA to provide revocation support for the Digital Certificate,
- Issuer CAs right to issue Digital Certificate expires or is revoked or terminated,
- Issuer CAs Private Key for the relevant issuing CA Certificate is compromised,
- Issuer CAs receive notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Issuer CAs jurisdiction of operation,
- The continued use of the certificate is harmful to the business of Issuer CAs and their relying parties.

When considering whether certificate usage is harmful, Issuer CAs should consider, amongst other things, the following:

- The nature and number of complaints received,
- The identity of the complainant(s),
- Relevant legislation in force, and
- Responses to the alleged harmful use from the Subscriber.

Issuer CAs that cross sign other issuer CAs may revoke the Issuing CA:

- If the cross signed Issuer CA no longer meets the contractual terms and conditions of the agreement between the two parties,

4.9.2 Who Can Request Revocation

Issuer CAs and RAs shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the certificate. Issuer CAs may also at their own discretion revoke certificates including certificates that are issued to other cross signed Issuer CAs.

4.9.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, Issuer CAs and RAs may provide automated mechanisms for requesting and authenticating revocation requests. For example through an account which issued the certificate to be revoked. RAs may also provide manual backup processes in the event that automated revocation methods are not possible.
Issuer CAs and RAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the certificate if the request is authentic and approved.
Once revoked, the serial number of the certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs may be published immediately or they may be published as defined within the Issuer CA's CPS.

4.9.4 Revocation Request Grace Period

The 'revocation request grace period' is the time available for a Subscriber to take any necessary actions themselves in order to request revocation of a suspected key compromise, use of a weak key or discovery of inaccurate information within an issued certificate. Issuer CAs should allow subscribers a maximum of 48 hours to take appropriate action to revoke or take appropriate action on behalf of Subscribers.

4.9.5 Time Within Which CA Must Process the Revocation Request

Issuer CAs shall begin investigation procedures for a suspected key compromise or misuse of a certificate within 24 (twenty-four) hours of receipt of the report.

All revocation requests for End Entity Certificates, both those generated automatically via user accounts and those initiated by the Issuer CA itself must be processed within a maximum of 30 minutes of receipt.

Issuer CAs that cross sign other CAs should process a revocation request within 24 hours of a confirmation of compromise and a ARL should be published within 12 hours of any off-line ARL key ceremony.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying upon a certificate, relying parties must validate the suitability of the certificate to the purpose intended as well as ensuring the certificate is valid. Relying parties will need to consult CRL or OCSP information for each certificate in the chain as well as validating that the certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). Issuer CAs may include all applicable URLs within the certificate to aid relying parties perform the revocation checking process.

4.9.7 CRL Issuance Frequency

All Issuer CAs must meet the requirements of the CABForum Base Requirements for Publically Trusted Certificates and/or the CABForum Requirements for Extended SSL certificates. In addition Issuer CAs that operate offline shall publish a CRL every 6 months. Issuer CAs that operates online must publish CRLs at least every 24 hours.

4.9.8 Maximum Latency for CRLs

Issuer CAs should ensure that online CRLs are published every 3 hours. A request for revocation received from an RA during the 3 hour period prior to the next scheduled CRL should be included within the CRL if received up to 30 minutes prior.
Issuer CAs that cross sign other CAs should revoke within 24 hours of a confirmation of compromise and a ARL should be published within 12 hours of the key ceremony.

4.9.9 On-Line Revocation/Status Checking Availability

Issuer CAs that support OCSP responses in addition to CRLs shall provide response times no longer than 10 seconds under normal network operating conditions.

4.9.10 On-Line Revocation Checking Requirements

Relying parties must confirm revocation information.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

Issuer CAs and related registration authorities shall use commercially reasonable methods to inform subscribers that their private key may have been compromised. This includes cases where new vulnerabilities have been discovered or where the Issuer CA at their own discretion decides that evidence suggests a possible key compromise has taken place. Where key compromise is not disputed Issuer CAs shall revoke Issuing CA Certificates or Subscriber End Entity certificates and publish a revised CRL within 24 hours.

4.9.13 Circumstances for Suspension

Issuer CAs shall not support suspension

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Issuer CAs shall provide a certificate status service either in the form of a CRL distribution point or an OCSP responder or both.

4.10.2 Service Availability

Issuer CAs shall maintain 24x7 availability of certificate status services and may choose to use additional Content Distribution Network cloud based mechanisms to aid service availability.

4.10.3 Operational Features

No stipulation

4.10.4 End of Subscription

Subscribers may end their subscription to certificate services by having their certificate revoked or naturally letting it expire. Where Issuer CAs have issued Issuing CAs capable of end entity issuance contracts between parties must be maintained unless revocation is used to terminate the contract.

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed. An Issuer CA that offers Key Escrow Services to Subscribers may therefore escrow Subscriber Private Keys. Any keys which are escrowed must be held in at least the same level of security as when the keys were originally created.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

Issuer CAs shall have physical and environmental security policies for systems used for certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery, etc. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.1 Site Location and Construction

Issuer CAs shall ensure that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference and the protections provided should be commensurate with the identified risks in risk analysis plans.

5.1.2 Physical Access

Issuer CAs shall ensure that the facilities used for certificate life cycle management are operated in an environment that physically protects the services from compromise through unauthorized access to systems or data. An authorized employee should always accompany any unauthorized person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises shall be shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

Issuer CAs should ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

Issuer CAs should ensure that the CA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

Issuer CAs should ensure that the CA system is protected with a fire suppression system

5.1.6 Media Storage

Issuer CAs should ensure that any Media used is securely handled to protect it from damage, theft and unauthorized access. Media management procedures should be protected against obsolescence and deterioration of the media within a defined period of time and records are required to be retained. All media should be handled securely in accordance with requirements of the information asset classification scheme and media containing sensitive data must be securely disposed of when no longer required.

5.1.7 Waste Disposal

Issuer CAs should ensure that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

Issuer CAs should ensure that full system backups of the certificate issuance system are sufficient to recover from system failures and are made periodically (The period must be defined in the CPS). Back-up copies of essential business information and software must be taken regularly. Adequate back-up facilities must be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. At least one full backup copy must be stored at an offsite location (at a location separate from the certificate issuance equipment). Backups should be stored at a site with physical and procedural controls commensurate to that of the operational facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Issuer CAs should ensure that all operators and administrators including vetting agents are acting in the capacity of a Trusted Role. Trusted roles are such that no conflict of interest is possible and the roles are distributed such that no single person can circumvent the security of the CA system.

Trusted Roles include but are not limited to the following:

- **Security Officer/Head of Information Security:** Overall responsibility for administering the implementation of the security practices;
- **Administrator**: Approves the generation/revocation/suspension of certificates;
- **System Engineer**: Authorized to install, configure and maintain the CA systems used for certificate life cycle management;
- **Operator**: Responsible for operating the CA systems on a day to day basis. Authorized to perform system backup and recovery;
- **Auditor**: Authorized to view archives and audit logs of the CA trustworthy systems;
- **CA activation data holder**: authorized person that holds CA activation data that is necessary for CA hardware security module operation.
- **Vetting Agent**: Responsible for validating the authenticity and integrity of data to be included within digital certificates via a suitable RA system

5.2.2 Number of Persons Required per Task

Issuer CAs shall highlight the number of persons required per task within their CPS. The goal is to guarantee the trust for all CA services (key generation, certificate generation, revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a Trusted Role, issuer CAs shall run a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA. The CPS should describe the mechanisms that are used to identify and authenticate people appointed to trusted roles.

5.2.4 Roles Requiring Separation of Duties

Issuer CAs shall enforce role separation either by the CA equipment or procedurally or by both means. Individual CA personnel are specifically designated to the roles defined in section 5.2.1 above. It is forbidden to own at the same time the following roles:

- Security officer and System Engineer or Operator;
- Auditor and Security Officer or Operator or Administrator or System Engineer;
- System Engineer and Operator or Administrator.

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Issuer CAs shall employ a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. Issuer CA personnel should fulfil the requirement of *expert knowledge, experience and qualifications* through formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the Issuer CA's CPS, are documented in job descriptions. Issuer CA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Issuer CA personnel shall be formally appointed to trusted roles by senior management responsible for security.
The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

5.3.2 Background Check Procedures

All Issuer CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. Issuer CA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or another offence, which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed. Issuer CAs should require candidates to provide past convictions and turn down an application in case of refusal. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

5.3.3 Training Requirements

Issuer CAs ensure that all personnel performing duties with respect to the operation of the CA receive comprehensive training in:

- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform;
- Disaster recovery and business continuity procedures.

Issuer CA and RA personnel shall be retrained when changes occur in Issuer CA or RA systems. Refresher training shall be conducted as required and Issuer CA shall review refresher-training requirements at least once a year.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the Issuer CA or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

Issuer CAs should ensure that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions shall be applied to personnel violating provisions and policies within the CP, CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

Contractor personnel employed for Issuer CA operations must be subjected to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

Issuer CA should make available to its personnel this CP, any corresponding CPSs and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., Administrator Manuals, User Manuals, etc.) are provided in order for the trusted personnel to perform their duties.
Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the Issuer CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non- electronic, shall be retained and made available during compliance audits.
Issuer CAs should ensure all events relating to the life cycle of certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- The type of event,
- The date and time the event occurred,
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,
- The identity to which the event was targeted,
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs should be reviewed periodically and reasonably for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Audit log records must be held for a period of time as appropriate to providing necessary legal evidence in accordance with any applicable legislation. Records may be required at least as long as any transaction relying on a valid certificate can be questioned.

5.4.4 Protection of Audit Log

The events must be logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.
The events must be logged in a manner to ensure that only authorized trusted access is able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.
The events must be protected in a manner to keep them readable in the time of their storage.
The events must be date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed-up in a secure location (For example a fire proof safe), under the control of an authorized trusted role, separated from their component source generation. Audit log backup should be protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection systems may be an internal component. Audit processes must be invoked at system start up and may finish only at system shutdown. The audit collection system should ensure the integrity and availability of the data collected. If necessary, the audit collection system should protect the data confidentiality. In the case of a problem occurring during the process of the audit collection then Issuer CAs must determine whether to suspend Issuer CA operations until the problem is solved, duly informing the impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Issuer CAs shall perform regular vulnerability assessments covering all Issuer CA assets related to certificate issuance products and services. Assessments should focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

Issuer CAs and RAs should archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. At a minimum, the following data shall be archived:

CA key lifecycle management events, including:-

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle management events; and
- CA System equipment configuration.

CA issuance system management events including:-

- System start-up and shutdown actions;
- Attempts to create, remove, or set passwords or change the system; and
- Changes to Issuer CA keys.

CA and Subscriber Certificate lifecycle management events, including:-

- Certificate requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts;
- All verification activities stipulated in this CP;
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- Acceptance and rejection of Certificate requests;
- Issuance, revocation, expiration of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries including failed read-and-write operations on the certificate and CRL directory.

Security events, including:-

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Documentation and Auditing:-

- Audit documentation including all work related communications to or from Issuer CA and compliance auditors;
- Certificate Policy and previous versions;
- Certification Practice Statement and previous versions; and
- Contractual agreements between subscribers and the Issuer CA

Time stamping:-

- Clock synchronisation

Miscellaneous

- Other data or applications sufficient to verify archive contents;
- Equipment failure;
- UPS failure or Electrical power outages; and
- Violations of this CP or CPS.

5.5.2 Retention Period for Archive

The minimum retention period for archive data shall be 10 years.

5.5.3 Protection of Archive

The archives should be created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections should ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

No Stipulation.

5.5.5 Requirements for Time-Stamping of Records

If a time stamping service is used to date the records, then it has to respect the requirements defined in section 6.8. Irrespective of time stamping methods, all logs must have must have data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of Issuer CA archive information are checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.
Only authorised Issuer CA equipment, trusted role and other authorized persons are allowed to access the archive.

5.6 Key Changeover

Issuer CAs may periodically changeover Key Material for issuing CAs in line with section 6.3.2. Certificate subject information may be modified and certificate profiles may be altered to highlight new best practices. Keys used to sign previous Subscriber certificates shall be maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Issuer CAs shall establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the Issuer CA services. Issuer CAs should carry out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary *(threat evolution, vulnerability evolution etc).* This business continuity is in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan.
Issuer CA personnel that own a trusted role and operational role should be specially trained to operate according to procedures defined in the Disaster Recovery plan for the most sensitive activities.
If an Issuer CA detects a potential hacking attempt or another form of compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, the Issuer CA should assess the scope of potential damage in order to determine if the CA or RA system needs to be rebuilt, if only some certificates need to be revoked, and/or if a CA hierarchy needs to be declared as compromised. The CA disaster recovery plan should highlight which services should be maintained *(for example revocation and certificate status information).*

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If any equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate certificates status information according to the Issuer CA's disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In case an Issuer CA signature key is compromised, lost, destroyed or suspected to be compromised:

- The Issuer CA shall, after investigation of the problem decides whether the Issuer CA certificate should be revoked. If so, then:-
    - All the subscribers who have been issued a certificate will be notified at the earliest feasible opportunity;
    - A new Issuer CA key pair shall be generated or an alternative existing CA hierarchy shall be used to create new subscriber certificates;

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in section 5.7.1. Certificate Status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability (with a rate of 99.95% availability excluding planned maintenance operations).

5.8 CA or RA Termination

In the event of termination of an Issuer CA or RA, the Issuer CA shall provide notice to all customers prior to the termination and:

- Stops delivering certificates according to and referring to this CP

- Archive all audit logs and other records prior to termination;
- Destroys all private keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as another Issuer CA that delivers identical services;
- Use secure means to notify customers and software platform providers to delete all trust anchors.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Issuer CAs shall generate all issuing key pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. External witnesses (Ideally an independent auditor who normally performs audits on a regular basis) should be present and the ceremony, as a whole, must be video taped/recorded. Issuer CA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

Issuer CAs that create Private Keys on behalf of Subscribers may do so only when sufficient security is maintained within the key generation process through to any onward issuance process to the subscriber. This includes the ability to guarantee the integrity of the Key, the randomness of the Key material through a suitable RNG or PRNG and choice of a suitable encryption mechanism for transport of the Key to the Subscriber. Issuer CAs shall not archive private keys and must ensure that any temporary location of the key in any memory location during the generation process is purged.

6.1.3 Public Key Delivery to Certificate Issuer

Issuer CAs shall only accept Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public keys from Subscribers in line with section 3.2.1 of this CP.

6.1.4 CA Public Key Delivery to Relying Parties

Issuer CAs shall ensure that Public Key delivery to relying parties is undertaken in such as way as to prevent substitution attacks. This may include working with commercial browsers and platform operators to embed Root Certificate Public Keys into root stores and operating systems. Issuing CA Public Keys may be delivered via the Subscriber in the form of a chain of certificates or via a repository operated by the Issuer CA and referenced within the profile of the issued certificate.

6.1.5 Key Sizes

Issuer CAs shall follow NIST recommended timelines and best practice in the choice of Key material for Root CAs, Issuing CAs and end entity certificates delivered to subscribers. The same practice shall be contractually obligated to any Sub Issuing CAs outside of the direct control of the Issuer CA.

The following Key sizes and hashing algorithms may be used for Root Certificates, Issuing Certificates and End Entity Certificates and CRL/OCSP certificate status responders in line with CABForum Base Requirements and Extended Validation processes:-

- 2048 bit RSA key with Secure Hash Algorithm 1 (SHA-1)
- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)
- 256 bit ECDSA key with Secure Hash Algorithm 2 (SHA-256)
- 384 bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)

Where possible the entire certificate chain and any certificate status responses shall use the same level of security and cryptography. Exceptions due to cross-certified certificates are acceptable.

Certificates with an unsuitable cryptographic strength shall be replaced in sufficient time as to protect relying parties, Subscribers and Issuing CAs.

6.1.6 Public Key Parameters Generation and Quality Checking

Issuer CAs shall generate keys in accordance with FIPS 186 and shall use reasonable techniques to validate the suitability of keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Issuer CAs shall set Key Usage of certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (See section 7.1).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Issuer CAs shall ensure that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection. Issuer CAs that require Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection. This can be achieved for example though limitation to a suitable CSP (Cryptographic Service Provider) tied to a known FIPS compliant hardware platform as part of the enrolment process.

6.2.2 Private Key (n out of m) Multi-Person Control

Issuer CAs shall activate Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this private key multi-person controls are strongly authenticated (i.e. Token with PIN code).

6.2.3 Private Key Escrow

Issuer CAs shall not escrow Private Keys for any reason.

6.2.4 Private Key Backup

Issuer CAs shall back up private keys under the same multi-person control as the original Private Key for disaster recovery plan purposes.

6.2.5 Private Key Archival

Issuer CAs shall not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Issuer CA Private Keys must be generated, activated and stored in a Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they must be encrypted. Private Keys must never exist in plain text outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

Issuer CAs shall store Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

Issuer CAs are responsible for activating the private key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting private keys in line with the obligations that are presented in the form of a Subscriber Agreement or Terms of use Agreement.

6.2.9 Method of Deactivating Private Key

Issuer CAs shall ensure that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time an Issuer CA's Cryptographic Module is on-line and operational it is only used to sign certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, its Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

Issuer CA private keys must be destroyed when they are no longer needed or when the certificates to which they correspond have expired or are revoked. Destroying Private Keys requires Issuer CAs to destroy all associated CA secret activation data in such a manner that no information can be used to deduce any part of the private key.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Issuer CAs must archive Public Keys from certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Issuer CA certificates and renewed certificates shall have a maximum validity period of:-

- **Type Private Key Usage Certificate Term.**

• **Root Certificates[3] -**	20 years	30 years
• **TPM Root Certificates -**	30 years	40 years
• **Issuing CA -**	11 years	15 years
• **PersonalSign Certificates -**	No stipulation	5 years
• **Code Signing Certificates -**	No stipulation	3 years
• **EV Code Signing Certificates** -	No stipulation	39 months
• **DV SSL Certificates -**	No stipulation	5 years
• **AlphaSSL Certificates -**	No stipulation	5 years
• **OV SSL Certificates -**	No stipulation	5 years
• **EV SSL Certificates -**	No stipulation	27 months
• **Time Stamping Certificates -**	11 years	11 years
• **CA for AATL Certificates -**	No stipulation	5 years
• **PDF Signing Certificates -**	No stipulation	5 years
• **TrustedRoot**	No stipulation	10 years
• **NAESB Certificates-**	2 years	2 years

Issuer CAs must comply with the CABForum Minimum Guidelines for Publically Trusted SSL Certificates with respect to the maximum validity, therefore reducing the effective available certificate term.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of Issuer CA activation data used to activate Issuer CA private keys shall be made during a key ceremony (Refer to section 6.1.1). Activation data shall be generated automatically by the appropriate HSM and delivered to a shareholder who must be a person in trusted role. The delivery method must maintain the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issuer CA activation data must be protected from disclosure through a combination of cryptographic and physical access control mechanisms. Issuer CA activation data must be stored on smart cards.

6.4.3 Other Aspects of Activation Data

Issuer CA activation data must only be held by Issuer CA personnel in Trusted Roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions must be provided by the Operating System, or through a combination of Operating System, software, and Physical Safeguards. The Issuer CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide Discretionary Access Control;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide domain isolation for process;
- Provide self-protection for the operating system.

When Issuer CA PKI equipment is hosted on an evaluated platform in support of computer security assurance requirements then the system (Hardware, Software, Operating System), when possible, operates in an elevated configuration. At a minimum, such platforms use the same version of the computer operating system as that which received the evaluation rating. The computer systems are configured with the minimum of the required accounts, network services, and no remote login.

6.5.2 Computer Security Rating

All the Issuer CA PKI component software has to be compliant with the requirements of the protection profile from a suitable entity.

[3] *2048 bit keys Generated prior to 2003 using RSA may be used for 25 years due to limited usage due to key size restrictions within hardware, root stores and operating systems.*

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the Issuer CA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software developed are developed in a controlled environment, and the development process are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There is no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are obtained from sources authorized by local policy. Issuer CA hardware and software are scanned for malicious code on first use and periodically thereafter;
- Hardware and software updates are purchased or developed in the same manner as original equipment; and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the Issuer CA system as well as any modifications and upgrades are documented and controlled by the Issuer CA management. There is a mechanism for detecting unauthorized modification to the Issuer CA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the Issuer CA system. The Issuer CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

Issuer CA keeps watching on the maintenance scheme requirements to keep the level of trust of software and hardware that are evaluated and certified,

6.7 Network Security Controls

Issuer CA PKI components implements appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time-Stamping

All Issuer CA components are regularly synchronized with a time service such as an Atomic Clock or Network Time Protocol (NTP) Service. A dedicated authority (Time stamping authority) may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates;
- Issuance of Subscriber End Entity certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Issuer CAs shall issue digital certificates in compliance with X.509 Version 3

7.1.2 Certificate Extensions

Issuer CAs shall issue digital certificates in compliance with RFC 5280 and applicable best practice. Criticality shall also follow best practice and where possible prevent unnecessary risks to relying parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

Issuer CAs shall issue digital certificates with Algorithms indicated by the following OIDs

- **SHA1WithRSAEncryption** {iso(1) member - body(2) us(840) rsadsi (113549) pkcs(1) pkcs - 1(1) 5}
- **SHA256WithRSAEncryption** {iso(1) member - body(2) us(840) rsadsi (113549) pkcs(1) pkcs - 1(1) 11}
- **ECDSAWithSHA1** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) 1 }
- **ECDSAWithSHA224** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 1 }
- **ECDSAWithSH256** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 2 }
- **ECDSAWithSHA384** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 3 }
- **ECDSAWithSHA512** {iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 4 }

7.1.4 Name Forms

Issuer CAs shall issue digital certificates with Name Forms compliant to RFC 5280. Within the domain of each Issuing CA, Issuer CAs must include a unique non-sequential Certificate Serial Numbers that exhibits at least 20 bits of entropy.

7.1.5 Name Constraints

Issuer CAs may issue digital certificates with name constraints where necessary and mark as critical where necessary.

7.1.6 Certificate Policy Object Identifier

No stipulation

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Issuer CAs may issue digital certificates with a Policy Qualifier and suitable text

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

Issuer CAs shall issue Version 2 CRLs in compliance with RFC 5280

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

Issuer CAs may operate an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019

7.3.1 Version Number(s)

Issuer CAs shall issue Version 1 OCSP responses

7.3.2 OCSP Extensions

No stipulation

8.0 Compliance Audit and Other Assessments

The policies within this CP encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which Issuer CAs are required to operate. Issuer CAs that are not constrained by dNSNameConstraints are audited for compliance to one or both of the following standards:-

- AICPA/CICA WebTrust for Certification Authorities Version 1.0
- AICPA/CICA WebTrust for Extended Validation

8.1 Frequency and Circumstances of Assessment

Issuer CAs are required to maintain compliance (where products and services offered require compliance) via an independent auditor on at least an annual basis. The audit must cover the Issuer CA and its associated RA. This requirement is recursive through the hierarchy for all Issuer CAs that are not constrained by dNSNameConstraints. Constrained Issuer CAs are exempt from the independent audit but are not exempt from meeting the remaining requirements of policies identified within this CP.

8.2 Identity/Qualifications of Assessor

Applicable audits of Issuer CAs shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

Issuer CAs must choose an Auditor/Assessor who is completely independent from the Issuer CA.

8.4 Topics Covered by Assessment

The Audit must meet the requirements of the Audit scheme under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to the Issuer CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

Issuer CAs including cross signed issuing CAs that are not technically constrained must follow the same process if presented with a material non-compliance by external auditors must create a suitable corrective action plan to remove the deficiency.

8.6 Communications of Results

Results of the Audit must be reported to the CPS Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Issuer CAs may charge fees for certificate issuance or renewal. Issuer CAs may also charge for re-issuance or re-key. Fees and any associated terms and conditions should be made clear to Applicants.

9.1.2 Certificate Access Fees

Issuer CAs may charge for Access to any Database which stores issued certificates.

9.1.3 Revocation or Status Information Access Fees

Issuer CAs may charge additional fees to Subscribers who have a large relying party community and choose not to use OCSP stapling or other similar techniques to reduce the load on the Issuer CAs certificate status infrastructure.

9.1.4 Fees for Other Services

Issuer CAs may charge for other additional services such as Time Stamping.

9.1.5 Refund Policy

Issuer CAs may offer a refund policy to Subscribers. Subscribers who choose to invoke the refund policy should have all issued certificates revoked.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Issuer CAs that have no name constraints imposed on their issuing CA shall maintain Commercial General Liability insurance with policy limits of at least 2 million US dollars in coverage and Errors and Omissions / Professional Liability insurance with a policy limit of at least 5 million US dollars in coverage. The Issuer CA's insurance policies include coverage for (1) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (2) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, patent, and trademark infringement), invasion of privacy, and advertising injury. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

Issuer CAs may offer a Warranty Policy to Subscribers.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Issuer CAs shall define the scope of confidential information within its CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential within the CPS shall be deemed public. Certificate status information and certificates themselves are deemed public.

9.3.3 Responsibility to Protect Confidential Information

Issuer CAs shall protect confidential information. Issuer CAs shall enforce protection of confidential information through training and contracts with employees, agents and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Issuer CAs shall protect Personal Information in line with a Privacy Policy Published on a suitable repository along with this CP

9.4.2 Information Treated as Private

Issuer CAs shall treat all information received from Applicants that will not ordinarily be placed into a certificate as private. This applies both to those Applicants who are successful in being issued a digital certificate and those who are unsuccessful and rejected. Issuer CAs should periodically train all RA and Vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

9.4.3 Information Not Deemed Private

Certificate status information and any certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

Issuer CAs are responsible for securely storing Private Information in line with a published Privacy Policy document and may store information received in either paper or digital form. Any backup of Private Information must be encrypted when transferred to suitable backup media.

9.4.5 Notice and Consent to Use Private Information

Personal Information obtained from Applicants during the application and enrolment process is deemed private and permission is therefore required from the Applicant to allow the use of such information. Issuer CAs should incorporate the relevant provisions within an appropriate Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by the Issuer CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Issuer CAs may disclose private information without notice to Applicants or Subscribers where required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

Issuer CAs shall not knowingly violate the Intellectual Property Rights of third parties. Public and Private keys remain the property of Subscribers who legitimately hold them. Issuer CAs retain ownership of certificates however, they shall grant permission to reproduce and distribute certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Issuer CAs use this CP and applicable subscriber agreements to convey legal conditions of usage of issued 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 including the Issuer CA, any RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

9.6.1.1 CA Representations and Warranties for NAESB certificates

NAESB WEQ PKI requires that Issuer CAs must warrant that they have:-

- Issued, and will manage, the certificate in accordance with the NAESB WEQ PKI Standards.
- Complied with all requirements in this NAESB WEQ PKI Standards when identifying the Subscriber and issuing the certificate.
- That there are no misrepresentations of fact in the certificate actually known to or reasonably knowable by the RA and that the RA has verified information in the certificate.
- That information provided by the Applicant for inclusion in the certificate has been accurately transcribed in to the certificate.
- That the certificate meets the material requirements of the WEQ PKI standards.

9.6.2 RA Representations and Warranties

Issuer CAs require all RAs to warrant that they are in compliance with this CP and the relevant CPS and may choose to include additional representations within its CPS or RA agreement.

9.6.3 Subscriber Representations and Warranties

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 Issuer CAs.
- Ensuring that the public key submitted to the Issuer CA correctly corresponds to the private key used.
- Accepting all terms and conditions in any subscriber agreement, Issuer CA CP and associated policies published in the Issuer CAs repository.
- Refraining from tampering with an issued certificate.
- Using certificates only for legal and authorised purposes in accordance with this CP.
- Notifying the Issuer CA or RA of any changes in the information submitted.
- Ceasing to use a certificate if any featured information becomes invalid.
- Ceasing to use a certificate when it becomes invalid.
- Removing a certificate when invalid from any applications and/or devices they have been installed on.
- Using a 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 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 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 Issuer CAs in accordance with the requirements of this CP particularly with regards to registration.
- Only use the key pair for digital signatures and in accordance with any other limitations notified to the subscriber according to this CP or any Trusted Root CA Chaining agreement.
- Exercise absolute care to avoid unauthorized use of its private key.
- Use a key length and algorithm as indicated in this CP.
- Notify Issuer CAs 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 Pass Phrase)
      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 issuer CA must designate the usage of a trustworthy device as well as the choice of organizational context.

9.6.3.1 North American Energy Standards Board (NAESB) Subscribers

End Entities participating in the Business Practice Standard WEQ-012 v3.0 shall be required to be registered in the NAESB EIR and furnish proof that they are an entity authorized to engage in the wholesale electricity industry. Entities or organizations that may require access to applications using authentication specified under the NAESB Business Practice Standard WEQ-012, but do not qualify as a wholesale electricity market participant (e.g., regulatory agencies, universities, consulting firms, etc.) must register.

Registered End Entities and the user community they represent shall be required to meet to all End Entity obligations in these Business Practice Standards.
Each subscriber organization acknowledges their understanding of the following obligations to the WEQ 012 v3.0 PKI standard through GlobalSign CA as follows:-

Each End Entity organization shall certify to their certification entity that they have reviewed and acknowledge the following Business Practice Standard WEQ-012.

A. End Entity acknowledges the electric industry's need for secure private electronic communications that facilitate the following purposes:

    - Privacy: The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended;
    - Authentication: The assurance to one entity that another entity is who he/she/it claims to be;
    - Integrity: The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now"; and
    - Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message.

B. End Entity acknowledges the industry's endorsement of public key cryptography which utilizes public key Certificates to bind a person's or computer system's public key to its entity and to support symmetric encryption key exchange.

C. End Entity has evaluated each of its selected **C**ertificate **A**uthority's Certification Practices Statement in light of those industry standards as identified by the certificate authority.

End Entities shall be obligated to register their legal business identification and secure an "Entity Code" that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that End Entity.

End Entities shall also be required to comply with the following requirements:

- Protect their private keys from access by other parties.

- Identify, through the NAESB EIR, the specific entity they have selected GlobalSign to use as their Authorized Certification Authority
- Execute all agreements and contracts with the GlobalSign as required by GlobalSign's Certification Practices Statement necessary for the GlobalSign to issue Certificates to the End Entity for use in securing electronic communications.

- Comply with all obligations required and stipulated by the by GlobalSign in this certification practices agreement, e.g., certificate application procedures, Applicant identity proofing/verification, and certificate management practices.
- Confirm that it has a PKI certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to:
    - Certificate private key security and handling policy(ies)
    - Certificate revocation policy(ies)
- Identify the type of Subscriber (I.e., individual, role, device or application) and provide complete and accurate information for each Certificate request.

9.6.4 Relying Party Representations and Warranties

A party relying on an Issuer CA's certificate promises to:

- Have the technical capability to use digital certificates.
- Receive notice of the issuer CA and associated conditions for relying parties.
- Validate an Issuer CA's certificate by using certificate status information (e.g. a CRL or OCSP) published by the issuer CA in accordance with the proper certificate path validation procedure.
- Trust an Issuer CA's 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 an Issuer CA's 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 Issuer CA's certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

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

9.6.4.1 North American Energy Standards Board (NAESB) Relying Parties

Relying Party obligations shall be specified within the context of each NAESB requirement that employs these Business Practice Standards, in addition to the following:

- the Certificate was issued by GlobalSign, a registered Authorized Certification Authority;
- the entire Certificate validation/trust chain to the GlobalSign CA for NAESB issuing Authorized Certification Authority root Certificate is intact and valid;
- the Certificate is valid and has not been revoked and
- the Certificate was issued under one of the NAESB assurance level object identifiers

9.6.4.2 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Issuer CAs should make statements in their CPS that they do 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 a Warranty Policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.8 Limitations of Liability

The total liability of the Issuer CA should be limited in accordance with any Limited Warranty Policy and any limitations set forth in it's CPS.

9.8.1 Exclusion of Certain Elements of Damages

Issuer CAs should make statements in their CPS to the effect that in no event (except for fraud or wilful misconduct) is the issuer 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.

9.9 Indemnities

9.9.1 Indemnification by an Issuer CA

The Issuer CA's indemnification obligations need to be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including and Third Party Beneficiaries.

9.9.2 Indemnification by Subscribers

The Issuer CA shall include its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3 Indemnification by Relying Parties

The Issuer CA shall include its indemnification requirements for Relying Parties in its CPS.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

Issuer CAs should communicate the conditions and effect of this CP's termination via their appropriate repository.

9.11 Individual Notices and Communications with Participants

GlobalSign 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 section 2.2.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CP are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

Issuer CAs should post appropriate notice on their web sites of any major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

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.

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.

9.14 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.

9.15 Compliance with Applicable Law

GlobalSign complies with applicable laws of Belgium. Export of certain types of software used in certain GlobalSign 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.

9.16 Miscellaneous Provisions

9.16.1 Compelled Attacks

GlobalSign CA is subject to Belgium jurisdiction and regulatory framework. GlobalSign's CA infrastructure is based in Belgium and France, and RA infrastructure is based in Belgium and Japan. GlobalSign's sales offices and/or strategic partners have no access to any part of GlobalSign's CA infrastructure. GlobalSign will use all reasonable legal defence against being compelled by a third party to issue certificates in violation of the CP and CPS.

9.16.2 Survival

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

9.16.3 Entire Agreement

The Issuer CA will contractually obligate every RA involved with Certificate Issuance to comply with this CP and all applicable Industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.4 Assignment

Entities operating under this CP must not assign their rights or obligations without the prior written consent of GlobalSign

9.16.5 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 affect the original intention of the parties

9.16.6 Enforcement (Attorney's Fees and Waiver of Rights)

GlobalSign may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. GlobalSign's failure to enforce a provision of this CP does not waive GlobalSign's right to enforce the same provisions later or right to enforce any other provisions of this CP. To be effective any waivers must be in writing and signed by GlobalSign

9.17 Other Provisions

Third Party issuer CA's that want to subscribe to the TrustedRoot CA Chaining service of GlobalSign must adhere to this Certificate Policy, and all its conditions. This adherence is implemented and verified through a number of legal and procedural controls, and is verified through annual audits.
Controls include, but are not limited to:

- Execution of a CA Chaining agreement between TrustedRoot subscriber and GlobalSign.
- Submission and publication of Subscriber Certificate Practise Statement reviewed and acceptance by GlobalSign and/or GlobalSign auditors.
- Submission of PKI Infrastructure review by TrustedRoot subscriber and acceptance by GlobalSign and/or GlobalSign auditors.

9.17.1 CA Chaining Agreement

The CA Chaining Agreement includes the following, contractually enforceable, terms and conditions. Breach of any of these points, discovered by a GlobalSign and/or GlobalSign auditors, can lead to CA revocation.

- Use of TrustedRoot by Subscriber's enterprise and subsidiaries (50+% controlling interest) only.
- Non-commercial use only: certificates issued are for own use, staff, and third parties affiliated with Subscriber for existing business use and processes only. Reselling is explicitly disallowed.
- Restriction of types of end-entity certificates: S/MIME, SSL client and SSL server certificates.
- Requirement of submission of Certificate Practice Statement reviewed and accepted by GlobalSign.
- Compliancy with this Certificate Policy.
- Submission of PKI Infrastructure review documenting physical, personnel, network, logical and operational controls in line with industry standards.
- Requirement of FIPS 140-3 or equivalent cryptographic modules for CA and SubCA private key management.
- No cross-signing allowed.
- Enforcement of export controls for issued certificates in line with US Export regulations.
- Acceptance of annual audits by GlobalSign and/or GlobalSign auditors.
- Ongoing requirement to notify GlobalSign of material changes in CA environment as reported in the PKI Infrastructure review and Certificate Practise Statement.
- Acceptance of Subscriber that GlobalSign might publish Subscriber CA in a GlobalSign repository.

9.17.2 PKI Infrastructure review

Execution of TrustedRoot Subscriber Agreement is subject to review and acceptance by GlobalSign and/or GlobalSign auditors of Subscriber PKI Infrastructure review.
This review documents Subscribers CA hierarchy and security measures taken. It includes, but is not limited to, the following subjects:

- Logical Security Measures implemented – including personnel matters and separation of Duty and dual control.
- Physical Security Measures implemented.
- Network Security Measures implemented,
- CA Hierarchy implemented.
- HSM type and serial numbers.

9.17.3 Subscriber CA implementation

GlobalSign enforces a mandatory test signing of a Subscriber CA with a GlobalSign test CA. GlobalSign test CA duplicates the GlobalSign Root CA but is identified as for testing purposes (CAT versus CA) and is

not distributed to third party applications. Only after successful test signing is Subscriber CA signed by GlobalSign Root CA.

9.17.4 Ongoing requirements and audits

Subscriber must at all times adhere to its obligations. Subscriber has an ongoing duty to report to GlobalSign and/or GlobalSign auditors of any changes previously reported in section. GlobalSign will instruct its Auditors, as part of its own WebTrust for CA audit, to audit annually the requirements as stated above and will in addition obtain from a independent third party offering web site scanning services a list of any publically available domains to ensure compliance.