GlobalSign Certificate Policy

Date: August 7th 2017

Version: v5.5

CPS Policy Authority

Digitally signed by CPS Policy Authority
Date: 2017.08.07 11:44:28 +09'00'

Table of Contents

Document History

Version	Release Date	Author(s)	Status + Description
V4.0	22/03/12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CA/BForum Baseline Requirements 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 CA/BForum Baseline Requirements support
V4.3	01/07/12	Steve Roylance	Additional CA/BForum Baseline Requirements
V4.4	15/03/13	Giichi Ishii Lila Kee	Extended validity period of PersonalSign, Administrative updates. Modification to NAESB Certificates incorporating WEQ-012 v 3.0 updates
V4.5	31/03/13	Giichi Ishii	Statement of compliance to CA/Browser Forum Baseline Requirements, EPKI specification update
V4.6	07/03/14	Carolyn Oldenburg	Administrative updates/clarifications Modified provisions to ensure compliance with CA/Browser Forum Baseline Requirements
V4.7	25/06/14	Giichi Ishii	Modified availability requirement and maximum process time for revocation Administrative update/clarifications
V4.8	02/09/14	Steve Roylance	Modifications to enhance the description of domain validation processes, highlighted by public review.
V4.9	05/03/15	Carolyn Oldenburg Steve Roylance Giichi Ishii	Modified maximum validity period of Code Signing certificate GlobalSign's new R6 root and readability enhancements to cover new AATL offerings
V5.0	15/08/15	Steve Roylance	Policy OIDs and Publication of all of GlobalSign's Non Constrained Subordinate CAs
V5.1	02/05/16	Giichi Ishii Lila Kee	Annual Review Modified NAESB EIR requirements to reflect non WEQ energy participants requirements
V5.2	16/06/16	Steve Roylance	Adding Root R7 and R8 Certificates
V5.3	11/08/16	Giichi Ishii	Adding Test CA OID Reflected changes from CABF Ballot 173 Clarification on Certificate Transparency
V5.4	02/02/17	Giichi Ishii	Removal of Root R2 & R4; addition of code signing minimum requirements
V5.5	07/08/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie	Updates for AATL Digital Signing Service Added CAA record checking requirement Annual update/review to fix bugs

Acknowledgments

This GlobalSign CA CP conforms to:

- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- North American Energy Standards Board (NAESB) Accreditation Requirements for Authorized Certificate Authorities

This CP conforms to current versions of the requirements of the following schemes:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates

- CA/B Forum Network and Certificate System Security Requirements
- CA/B Forum EV Code Signing Certificate Guidelines
- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

  If there is any inconsistency between this document and the above Requirements, the Requirements take precedence over this document..

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 Certificates including validity checking services. GlobalSign nv/sa may also provide additional services such as timestamping. 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 of this CP, however, in the event of any inconsistency, the English version shall control).*

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 of GlobalSign's practices and procedures. GlobalSign CAs conform to the current version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the "Baseline Requirements"), the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (the "EV Guidelines"), CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (the "EV Code Signing Guidelines"), published at www.cabforum.org, and the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, published at https://aka.ms/csbr (the "Code Signing Minimum Requirements"). In the event that a discrepancy arises between interpretations of this document and the Baseline Requirements, the Baseline Requirement shall take precedence over this document. Additional assertions on standards used in this CP can be found under the *"Acknowledgements"* section 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 practices 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 Subordinate/Issuing CAs. Root Certificates are used to manage Certificate hierarchies through the creation of one or more Subordinate CAs that may or may not be controlled directly by the same entity that manages the Root Certificate itself.

This CP is final and binding between GlobalSign nv/sa, a company under public law, with a registered office at Martelarenlaan 38, 3010 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.

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 Trusted Root™ *(Previously known as Root Sign)* program including self-signed Root Certificates and Key Pairs. The purpose of this CP is to present GlobalSign CA's 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 (the "Law") provides for the recognition of electronic signatures that are used for the purposes of authentication or nonrepudiation. 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 CP. 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 Issuing CA *(i.e. the entity which provides the Subscriber its Certificate)* will use in creating and managing such Certificates. Likewise, GlobalSign CA Trusted Root Subscribers who themselves become an *Issuing CA* maintain their own Certificate Practice Statement applicable to products and services they offer.

In addition to this CP and the CPS, GlobalSign maintains additional documented policies which address such issues as:

- Business continuity and disaster recovery
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

Additionally, other relevant documents include:

- The GlobalSign Warranty Policy that addresses issues on insurance;
- The GlobalSign Privacy Policy on the protection of personal data; and
- 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 are subject to audit by authorised third parties which GlobalSign CA highlights on its public facing web site via a WebTrust Seal of Assurance. Additional information can be made available upon request.

The exact names of the GlobalSign CA Certificates are governed by this CP are: -

GlobalSign Public Root CA Certificates: -

- GlobalSign Root CA – R1 with serial number 040000000001154b5ac394
- GlobalSign Root CA – R3 with serial number 04000000000121585308a2
- GlobalSign Root CA – R5 with serial number 605949e0262ebb55f90a778a71f94ad86c
- GlobalSign Root CA – R6 with serial number 45e6bb038333c3856548e6ff4551
- GlobalSign Root CA – R7 with serial number 481b6a06a6233b90a629e6d722d5
- GlobalSign Root CA – R8 with serial number 481b6a09f4f960713afe81cc86dd

Non-public Root Certificates: -

- GlobalSign Non-Public Root CA – R1 with serial number 467437789376ad2301cdf9ba9e1d
- GlobalSign Non-Public Root CA – R3 with serial number 4674377c0fba34f6f1c3dcb75d3f

GlobalSign CA actively promotes the inclusion of the five Root Certificates above into hardware and software platforms that are capable of supporting 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. Roots R2 & R4 are no longer owned by GlobalSign nv-sa.

Trusted Root 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 040000000001201909l9AE
- GlobalSign Trusted Platform Module ECC Root CA with s/n 45dc9c8c1515db59d0464b9d79e9[1]

Trusted Root TPM is the GlobalSign service which allows third party Issuing CAs to chain to one of the GlobalSign Trusted Platform Module Root CA Certificates above.

Certificates allow entities that participate in an electronic transaction to prove their identity to other participants or sign data digitally. By means of a Certificate, a Certification Authority provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. For Trusted Root CA's, the purpose of entering the GlobalSign hierarchy is to enhance trust in an Issuer CA's own hierarchy, as well as providing greater functionality within third party applications such as web browsers. It is the duty of any Trusted Root Issuer CA to assess the value of the GlobalSign services at any point in time and act accordingly.

[1] *Collectively Root R1,3,5,6,7,8 and the TPM/TPM ECC Roots are referred to as the GlobalSign CA Root Certificates*

The process to obtain a 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 confirmation of the identity of the Subject of a Certificate by binding the Public Key the Subscriber uses through the issuance of a Certificate. An entity in this instance might include an end user or another Certification Authority. GlobalSign CA makes available 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 or transaction level in support of a warranty policy or other limitations imposed by the applications that Certificates are used in.

GlobalSign CA accepts comments regarding this CP addressed to the address stated in Section 1.5, *Policy Administration.*

1.1.1 Additional requirements for Trusted Root Issuer CAs

This CP also addresses the Trusted Root program for authorized Issuing CAs. Entering the GlobalSign CA hierarchy is carried out through a CA chaining program that GlobalSign CA makes available to interested parties under the Trusted Root brand. Trusted Root CA Certificates are typically: -

- Issued by GlobalSign CA to a third party Issuing CA that meets the contractual, audit and policy requirements of GlobalSign CA Trusted Root 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 to 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; and
- Constrained to specific domains for either SSL and/or S/MIME usage to protect both the third party and GlobalSign hierarchy.

GlobalSign CA expressly forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection.

1.2 Document Name and Identification

This document is the GlobalSign CA Certificate Policy.

The OID for GlobalSign nv/sa is an 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:

Extended Validation

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

Domain Validation

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

Organization Validation

1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy

Intranet Validation

1.3.6.1.4.1.4146.1.25	IntranetSSL Validation Certificates Policy

Time Stamping

1.3.6.1.4.1.4146.1.30	Time Stamping Certificates Policy
1.3.6.1.4.1.4146.1.31	Time Stamping Certificates Policy – AATL

Client Certificates

1.3.6.1.4.1.4146.1.40	Client Certificates Policy (Generic)
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)
1.3.6.1.4.1.4146.1.40.30	Client Certificates Policy (AATL)
1.3.6.1.4.1.4146.1.40.40	Client Certificates Policy (ePKI for private CAs)

Code Signing

2.23.140.1.4.1	Code Signing Minimum Requirements
1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy

Certificates issued by GlobalSign containing this OID are issued and managed in accordance with the Code Signing Minimum Requirements.

CA Chaining and Cross Signing

1.3.6.1.4.1.4146.1.60	CA Chaining Policy – Trusted Root and Hosted Root
1.3.6.1.4.1.4146.1.60.1	CA Chaining Policy – Trusted Root (Baseline Requirements Compatible)

Others

1.3.6.1.4.1.4146.1.21	Test OneClick Certificate Policy
1.3.6.1.4.1.4146.1.26	Test Certificate Policy (Should not be trusted)
1.3.6.1.4.1.4146.1.70	High Volume CA Policy
1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90	Trusted Root TPM Policy
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy

In addition to these identifiers, all Certificates that comply with the NAESB Business Practice Standards will include one of the following additional identifiers: -

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 Baseline Requirements will include the following additional identifiers: -

2.23.140.1.1	Extended Validation Certificate Policy
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 tasks related to Public Key Infrastructure (PKI) functions such as Certificate lifecycle management, Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. Certificate status information may be provided using a Repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) 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 a Registration Authority (RA) from a Subordinate CA which may or may not be managed by GlobalSign CA (i.e. a Trusted Root Issuing CA).

The GlobalSign CA Policy Authority, which is composed of members of the GlobalSign management team and appointed by its Board of Directors, is responsible for maintaining this Certificate Policy relating to all Certificates in the GlobalSign hierarchy. Through its Policy Authority, GlobalSign CA has ultimate control over the lifecycle and management of the GlobalSign Root CA and any subsequent Subordinate CAs including Trusted Root Issuing 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 for GlobalSign CA on the basis of a service agreement. The scope of the outsource services provided is Certificate issuance and revocation services. The GlobalSign CA outsource 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 certain services and Certificates on behalf of GlobalSign CA.

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

Issuing CAs ensure 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. Issuing CAs provide Certificate status information using a Repository in the form of a CRL distribution point and/or OCSP responder as indicated within the Certificate properties.

1.3.2 Registration Authorities

In addition to identifying and authenticating Applicants for Certificates, an RA may also initiate or pass along revocation requests for Certificates and requests for re-issuance and renewal (sometimes referred to as re-key) of Certificates. Issuing CAs may act as a Registration Authority for Certificates they issue 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 an Applicant's application;
- Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and
- Initiating the process to revoke a Certificate from the applicable GlobalSign Subordinate CA or partner Subordinate 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 comply with all the requirements of this CP and the terms of their contract which may also refer to additional criteria as recommended by the CA/BForum. RA's may implement more restrictive vetting practices if their internal policy dictates.

In order to issue certain Certificate types, RAs may need to rely on Certificates issued by third party Certification Authorities or other third party databases and sources of information Such as government national identity cards such as passwords, eID, and drivers' licenses. Where the RA relies on Certificates issued by third party Certification Authorities, Relying Parties are advised to review additional information by referring to such third party's CPS.

Issuing CAs may designate an Enterprise RA to verify Certificate Requests from the Enterprise RA's own organization. In Enterprise RA, the Subscriber's organization shall be validated and pre-defined, and shall be constrained by system configuration.

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 Entities or natural persons 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.

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 Trusted Root services with regard to operational practices and technical implementation:
- Can only be enterprise in-house PKI's. No public PKI services are allowed; and
- 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 the Subject of the following Certificates:

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

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

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

Legal Entities created through all recognized forms of incorporation or government entities can be listed as the Subject of the following Certificates:

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

Legal Entities or self-employed professionals can be listed as the Subject of the following Certificates:

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

DNS Names may be listed as the Subject of the following Certificates.

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

RFC822 email addresses may be listed as the Subject of the following Certificates.

- **PersonalSign 1**

1.3.4 Relying Parties

Business partners of a Trusted Root partner that receive S/MIME Certificates issued by the Trusted Root Subscriber's CA are effectively Subscribers and Relying Parties at the same time.

To verify the validity of a 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 Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. 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 Trusted Root program can be used to issue Certificates for transactions that require:

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

Additional uses are specifically designated once they become available to end entities. Unauthorised use of Certificates may result in the voiding 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 GlobalSign 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 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, and
  - 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.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

GlobalSign NV
Policy Authority 2
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

Policy Authority 2 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 a Qualified Auditor.

In an effort to maintain credibility and promote trust in this CP and better correspond to accreditation and legal requirements, the Policy Authority shall review this CP at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CP.

1.5.4 CP Approval Procedures

Policy Authority 2 reviews and approves any changes to the CP. Upon approval of a CP update by the Policy Authority, the new CP is published in the GlobalSign Repository at https://www.globalsign.com/repository.

The updated version is binding upon all Subscribers including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CP.

1.6 Definitions and acronyms

Any terms used but not defined herein shall have the meaning ascribed to them in the the Baseline Requirements, the EV Guidelines, and/or the EV Code Signing Guidelines.

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.

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 Identity Information is correct.

Business Entity: Any entity that is not a Private Organization, Government Entity, or non-commercial entity as defined in the EV Guidelines. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

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

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom GlobalSign CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

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: A 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 of the Baseline Requirements requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated timestamped 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.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

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

Domain Name System: An Internet service that translates *Domain Names* into IP addresses.

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).

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization or its subsidiaries. An Enterprise RA may also authorize issuance of client authentication Certificates to partners, customers, or affiliates wishing to interact with that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.

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

Governmentally Accepted Form of ID: A physical or electronic form of ID issued by the local country/state government, or a form of ID that the local government accepts for validating identities of individuals for its own official purposes. **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.

Hardware Security Module (HSM): 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.

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.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Individual: A natural person.

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.

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

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) Accreditation Requirements for Authorized Certification Authorities ("NAESB Accreditation Specification"): 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.

NAESB Business Practice Standards for Public Key Infrastructure (PKI) – WEQ-012 ("NAESB Business Practice Standards"): Defines the minimum requirements that must be met by Certification Authorities, the Certificates issued by those Certification Authorities and end entities that use those Certificates in order to comply with NAESB PKI standards.

Object Identifier (OID): 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.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

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 (PKI): 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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).

Qualified Government Information Source: A database maintained by a Government Entity

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

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.

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.

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 Agreement or Terms of Use.

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 the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Trusted Third Party: A service provider with a secure process used for individual identity verification based on Governmentally Accepted Form(s) of ID, or whose service itself is considered to generate a Governmentally Accepted Form of ID.

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.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

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

Vetting Agent: 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 Certificates.

AATL	Adobe Approved Trust List
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
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
EIR	Electric Industry Registry
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEdu	A Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
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
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
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
WEQ	Wholesale Electric Quadrant

2.0 Publication and Repository Responsibilities

2.1 Repositories

The Issuing CA shall publish all CA Certificates and Cross Certificates issued to and from the Issuing CA, revocation data for issued Certificates, CP, CPS, and Relying Party agreements and Subscriber Agreements in Repositories. The Issuing CA shall ensure that revocation data for issued Certificates and its Root Certificate 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 downtime that does not exceed 0.5% annually.

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

Issuing CAs may refrain from making publicly available certain sensitive and/or confidential documentation including security controls, operating procedures, and internal security policies. These documents are, however, made available to Qualified Auditors as required during any WebTrust or ETSI audit performed on GlobalSign CA.

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 in the event of any inconsistency, the English version shall control.

2.2 Publication of Certificate Information

Issuing CAs shall make publically available this CP and any CPS, CA Certificates, Subscriber Agreements, Relying Party agreements, and CRLs in Repositories. CRLs should contain entries for all revoked unexpired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain. Issuing CAs may choose to maintain the serial numbers of expired Certificates on a CRL to further promote additional security.

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 24 hours. CRLs for CA Certificates are issued at least every 3 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

GlobalSign CA reviews their CP and CPS at least annually and makes appropriate changes so that GlobalSign CA operation remains accurate, transparent and complies with external requirements listed in the "*Acknowledgements*" section of this document. New or modified versions of this CP, the CPS, Subscriber Agreements, or Relying Party agreements 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 Issuing 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

Issuing CAs maintain documented practices and procedures to authenticate the identity and/or other attributes of the Applicant.

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

Issuing CAs must authenticate the requests of parties wishing to perform revocation of Certificates under this CP.

3.1 Naming

3.1.1 Types of Names

To identify a Subscriber, Issuing 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, Issuing CAs shall use distinguished names to identify both the Subject and issuer name 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

Issuing CAs may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and 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

Issuing 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. This CP does not require that an Applicant's right to use a trademark be verified. However, Issuing CAs may reject any applications or require revocation of any Certificate that is part of a dispute.

3.2 Initial Identity Validation

Issuing CAs may perform identification of the Applicant or for services including CA chaining services using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

Issuing 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 provided that the re-verification requirements of Section 3.3.1 are complied with.

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 Certificate Signing Request (CSR) in addition to an out-of-band confirmation.

Issuing CAs may accept other Issuing CAs wishing to enter their hierarchy through the Trusted Root program. Following an initial assessment and signing of a specific agreement with the Issuing CA, the applicant Subordinate CA must also prove possession of the Private Key. CA chaining services do not mandate the physical appearance of the Subscriber representing the Subordinate CA so long as an agreement between the applicant organisation (which has been authenticated) and the Issuing 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 (where included in the request or part of the legal name in the jurisdiction of incorporation) and provided address of the organization must be verified and any methods used must be highlighted in the CPS.

The authority of the Applicant to request a Certificate on behalf of the organization must be verified in accordance with Section 3.2.5.

3.2.2.1 Local Registration Authority Authentication

For accounts that allow the concept of a Local Registration Authority, Issuing CAs and RAs may set 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 with the organization and/or any sub-domains owned or controlled by the organization. (Whilst LRA's are able to authenticate individuals under contract, all Domain Names to be authenticated must have previously had the appropriate higher-level Domain Name pre-authorized and authenticated in compliance with this CP and the Baseline Requirements).

3.2.2.2 Machine, Device, Department, and Role based Certificate Authentication (DepartmentSign)

Issuing CAs must ensure that requests for machine, device, department, or role-based Certificates are authenticated either by a RA, acting on behalf of the CA, or a LRA that is contractually obligated to the Issuing CA/RA to ensure that machine, device, department, or role-based names relating to the organization and its business are accurate and correct.

3.2.3 Authentication of Individual identity

Issuing CAs or RAs shall authenticate individuals depending upon the class of Certificate as indicated below.

3.2.3.1 Class 1

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

3.2.3.2 Class 2

The Applicant is required to demonstrate control of the identity attributes included in the request, such as their email address or domain name to which the Certificate relates.

The Applicant is required to submit a legible copy of a valid government issued national identity document or photo ID (driver's licence, military ID or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. Issuing 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.

Issuing 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 telephone number from a reliable source;
- Performing a fax challenge/response to the Applicant using a fax number from a reliable source; or
- Performing an email challenge/response to the Applicant using an email address from a reliable source; or
- Performing a postal challenge to the Applicant using an address obtained from a reliable source;
- Receiving an attestation from an appropriate notary, Trusted Third Party that they have verified the individual, or identity based on a Governmentally Accepted Form of ID;
- In the case of individuals affiliated with an organization, GlobalSign may rely on attestations from the approved Local RA. Refer to 3.2.3.4 in case of a Class 2 Certificate requested through an EPKI or an MSSL profile;
- Receiving an attestation from a client to validate the identities of its own end customers based on a verification of a Governmentally Accepted Form of ID, while the client maintains a secure auditable trail of these verifications.
- 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.

In an email address is to be included in the

3.2.3.3 Class 3

For EV Code Signing, the Applicant is required to demonstrate control of any email address to be included within a Certificate.

For ExtendedSSL, the Applicant is required to demonstrate control of all domain names to be included in a Certificate.

The Applicant is required to submit a legible copy of a valid government issued national identity document or photo ID (driver's licence, military ID or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. Issuing 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.

For PersonalSign 3 Pro, 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.

Issuing CA or RAs are also required to authenticate the Applicant's authority to represent the organization wishing to be named as the Subject in the Certificate, using reliable means of communication, verified by GlobalSign as a reliable way of communicating with the Applicant in accordance with the EV Guidelines and the EV Code Signing Guidelines.

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 pre-vetted Organization accounts that allow the concept of a Local Registration Authority, Issuing CAs and RAs may set authenticated organizational details in the form of a *Profile.* Certificates issued within these accounts are populated with data fields from the profile. Suitably authenticated account administrators acting in the capacity of a Local Registration Authority must authenticate individuals affiliated with the organization.

3.2.3.5 North American Energy Standards Board (NAESB) Certificates

For NAESB Certificate Requests, authenticity of organization identity requests for Certificates in the name of an affiliated organization shall include the organization name, address, and documentation of the existence of the organization. GlobalSign or the 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 if using certificate for WEQ-012 applications 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.

When issuing certificates for use within the energy industry for other than WEQ-012 applications, ACAs must comply with: the provisions of the NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models, except provisions in WEQ-012-1.9.1, WEQ-012-1.3.3, and WEQ-012-1.4.3, which require End Entity registration within the NAESB EIR.

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 via on of its managed service offerings. 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 CP and the NAESB Accreditation Specification and NAESB Business Practice Standards. 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 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. The process shall depend

upon the Certificate level of assurance and shall be addressed in the NAESB Accreditation Specification. The documentation and authentication requirements shall vary depending upon the level of assurance.

Registration of Identity Proofing Requirements shall use 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 identification information supplied by the Applicant in compliance with the authentication requirements defined by NIST SP800-63 version 1.0.2 found at http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

3.2.4 Non Verified Subscriber Information

Issuing 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. Issuing CAs may use the Subject:organizationalUnitName as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices. In the case of individuals, a unique identifier such as mobile number may be used in conjunction with the individual's legal name.

- For all Certificate types where the Issuing 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 Issuing CA must verify the information and may therefore omit a disclaimer notice.

- For all Certificate types where the Issuing CA cannot explicitly verify the identity, e.g. a generic term such as "Marketing", then the Issuing CA may omit the disclaimer that this item is classified as non-verified Subscriber information as described herein. For IntranetSSL Certificates only, Issuing 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. The Baseline Requirements define a time frame for an industry wide sunset by which time these objects may no longer be included within Certificates. Until such time, these items are classified as non-verified Subscriber information as ownership cannot reasonably be validated.

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 email address to be listed within the Certificate through a challenge response mechanism.
PersonalSign Demo Certificates	Verification that the Applicant has control over the email address to be listed within the Certificate.
PersonalSign2 Certificates	Verification through a reliable means of communication with the individual Applicant together with verification that the Applicant has control over any email address included.
Noble Energy Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included
NAESB Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included (see Section 3.2.3.5.)
PersonalSign2 Pro	Verification through a reliable means of communication with the individual Applicant together with verification that the Applicant has

	control over the email address included if required. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
PersonalSign2 Department Certificates	Verification through a reliable means of communication with the individual Applicant together with verification that the Applicant has control over the email address if an email address is requested to be included in the Certificate. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
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 email address to be listed within the Certificate.
Code Signing Certificates	Verification of Organization and Individual Applicants in accordance with the Code Signing Minimum Requirements.
EV Code Signing Certificates	Verification of the authority of the contract signer and Certificate approver in accordance with the EV Guidelines and EV Code Signing Guidelines.
DV/AlphaSSL Certificates	Validation of the ownership or control of the domain name by a suitable challenge response mechanism. Either: - ▪ Using GlobalSign's OneClickSSL protocol whereby the Applicant is required to demonstrate control of a domain by installing a non-publicly trusted test Certificate of GlobalSign CA's design, ▪ By uploading specific metadata to a defined page on the domain, ▪ By direct confirmation with the contact listed with the Domain Name Registrar, ▪ Successfully replying to a challenge response email sent to one or more of the following email addresses: • webmaster@domain.com, postmaster@domain,admin@domain.com administrator@domain.com, hostmaster@domain, or • any address listed as a contact field of the WHOIS record. If the Country code is included within the DN then GlobalSign validates the Country based on the geo-location of the IP address obtained by a DNS query.
OV SSL & ICPEdu 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 via the methods listed in section 3.2.7. For Certificates issued through an MSSL account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
EV SSL Certificates	Verifying the authority of the contract signer and Certificate approver in accordance with the EV Guidelines together with verification that the Applicant has ownership or control of the domain name via the methods listed in section 3.2.7. For Certificates issued through an MSSL account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
Time Stamping Certificates	Verification through a reliable means of communication with the organization's Applicant.
AATL and CDS	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over the email address if an email address is requested to be included in the Certificate. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
Trusted Root	Verification through a reliable means of communication with the organization's Applicant and verification of all elements included within 'Name Constraints' which may include top level e-mail domain/sub domain names or domain names as detailed in section 3.2.7.

3.2.6 Criteria for Interoperation

Not applicable

3.2.7 Authentication of Domain Name

For all SSL/TLS Certificates, the Applicant's ownership or control of all requested Domain Name(s) and IP address must be verified with methods to achieve this in accordance with the Baseline Requirements section 3.2.2.4 and must be detailed within the CPS.

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.

3.2.8 Authentication of Email addresses

GlobalSign must uses the following methods to confirm that the Applicant has control of or right to use email addresses:

1. Having the Applicant demonstrate control over the email address via a challenge/response; or
2. Having the Applicant demonstrate control over or right to use the FQDN using one of the Domain Validation processes listed above. Once verified, an Enterprise RA can issue certificates containing email addressed under that FQDN.

3.3 Identification and Authentication for Re-key Requests

Issuing CAs may support re-key requests from Subscribers prior to the expiry of the Subscriber's existing Certificate. Issuing CAs may also support reissue at any time during the lifetime of the Certificate. Re-issue is a form of re-key, 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 reissued.

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
- **Noble Energy 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 & ICPEdu 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
- **Trusted Root** 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 Private Key.
Basic	Identity may be established through use of current Private 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 Private 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 Private Key, except that identity shall be established through initial registration process at least annually.

3.3.2 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 CP to obtain a new Certificate.

3.3.3 Re-verification and Revalidation of Identity When Certificate Information Changes

If at any point any Subject name information embodied in a Certificate is changed in any way, the identity proofing procedures outlined in this requirement must be re-performed and a new 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.

3.3.4 Identification and Authentication for Re-key After Revocation

A routine re-key after revocation is not supported. Re-key after revocation of a Certificate requires the Subscriber to follow the initial validation process that was previously 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 Issuing CA. Revocation requests from Subscribers may be granted following a suitable challenge response such as logging into an account with a username and password, or proving possession of unique elements incorporated into the Certificate, e.g. Domain Name or email address.

Issuing CAs may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non- payment of applicable fees.

4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Issuing 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 recognized denied persons lists which are applicable to the jurisdictions in which the Issuing CA operates may be used to screen unwanted Applicants.

4.1.2 Enrollment Process and Responsibilities

Issuing CAs shall maintain systems and processes that sufficiently authenticate the Applicant's identify for all Certificate types that present the identity to Relying Parties. Applicants should submit sufficient information to allow Issuing CAs and RAs to successfully perform the required verification. Issuing CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Issuing CAs shall maintain systems and processes to sufficiently authenticate the Applicant's identify in in compliance with its CPS. Initial identity validation shall be performed by an Issuing CAs validation team or by Registration Authorities under contract as set forth in Section 3.2 of this CP. All communications shall be securely stored along with all information presented directly by the Applicant during the application process. Future identification of repeat Applicants and subsequent authentication checks may be addressed using single (username and password) or multi-factor (Certificate in combination with username/password) authentication principles.

GlobalSign shall validate each server FQDN in publicly trusted SSL certificates against the domain's CAA records. If a CAA record exists that does not list globalsign.com as an authorized CA, GlobalSign shall not issue the certificate.

CAA checking is optional for GlobalSign Trusted Root customers that issue SSL certificates using Name Constrained CAs.

4.2.2 Approval or Rejection of Certificate Applications

Issuing CAs shall reject applications for Certificates where validation of all items cannot successfully be completed.

Assuming all validation steps can be completed successfully following appropriate best practice techniques Issuing CAs shall generally approve the Certificate Request. Issuing CAs may reject applications including for the following reasons:

- Based on potential brand damage to GlobalSign CA in accepting the application.
- For Certificates from Applicants who have previously been rejected or have previously violated a provision of a Subscriber Agreement.

Issuing CAs are under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

4.2.3 Time to Process Certificate Applications

Issuing 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

Certificate issuance by GlobalSign Root CA requires an authorized Trusted Role member from GlobalSign to deliberately issue a direct command in order for the Root CA to perform a Certificate signing operation.
Issuing CAs shall communicate with any RA accounts capable of causing Certificate issuance using multi-factor authentication. RAs directly operated by the Issuing CA or RAs contracted by the Issuing 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 Issuing CA shall notify 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

Issuing CAs shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open ended stipulation, Issuing 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

Issuing CAs may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in a suitable Repository, including to Certificate Transparency Logs.

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. Issuing 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 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 Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

In the case of GlobalSign's Digital Signing Service, and with the consent of the Subscriber, GlobalSign shall host, secure, and manage short-lived Certificates and their corresponding Private Keys.

4.5.2 Relying Party Public Key and Certificate Usage

Issuing CAs must describe the conditions under which 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). Issuing 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 Certificate from the Issuing 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 exception of NAESB Certificates which must rely on re-keying but contains a new 'Not After' date. Issuing CAs that support renewal must identify the products and services under which renewals can be accepted. An Issuing 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; and
- All details within the Certificate remain accurate and no new or additional validation is required.

Issuing CAs may renew Certificates which have either been previously renewed or previously re-keyed (subject to the points above). The original Certificate may be revoked after renewal is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.6.2 Who May Request Renewal

An Issuing 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 Issuing 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 Issuing CAs may refer to this as reissue.

Issuing CAs that support re-keying must identify the products and services under which re-keys can be accepted. An Issuing 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; and
- All details within the Certificate remain accurate and no new or additional validation is required.

Issuing CAs may re-key Certificates which have either been previously renewed or previously re-keyed (subject to the points above). The original Certificate may be revoked after re-key is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.7.2 Who May Request Certification of a New Public Key

An Issuing 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 the Private Key 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 Issuing CA may request additional information before processing a re-key or reissue request and may re-validate the Subscriber subject to re-verification of any previously validated data. In the case of a reissuance, 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 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.

- Issuing CAs shall treat modification in the same was a 'New' issuance.
- Issuing CAs may modify Certificates that have either been previously renewed or previously re-keyed. The original Certificate may be revoked after modification is complete, however, the original Certificate must not be further renewed, re-keyed 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 Certificate Revocation List (CRL). The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding

a serial number allows Relying Parties to establish that the lifecycle of a Certificate has ended. Issuing CAs may remove serial numbers once a Certificate has normally expired to promote more efficient CRL file size management. Prior to performing a revocation Issuing CA's will verify the authenticity of the revocation request. Revocation of a Subscriber's Certificate shall be performed within twenty-four (24) hours under the following circumstances: -

- The Subscriber requests in writing (to the GlobalSign entity which provided the Certificate) that they wish to revoke the Certificate;
- The Subscriber notifies GlobalSign CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- GlobalSign CA obtains reasonable evidence that the Subscriber's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- GlobalSign CA receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;
- GlobalSign CA is made aware of any circumstance indicating that used of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- GlobalSign CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
- GlobalSign CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements or GlobalSign's CP or this CPS;
- If GlobalSign CA determines that any of the information appearing in the Certificate is not accurate or is misleading;
- GlobalSign CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- GlobalSign CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless GlobalSign CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- GlobalSign CA is made aware of a possible Compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
- Revocation is required by GlobalSign CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);

Revocation of a Subscriber Certificate may also be performed within a commercially reasonable period of time under the following circumstances: -

- The Subscriber or organization administrator requests revocation of the Certificate through a GCC account which controls the lifecycle of the Certificate;
- The Subscriber requests revocation of the Certificate via a OneClickSSL revocation workflow process;
- The Subscriber requests revocation through an authenticated request to GlobalSign CA's support team or GlobalSign CA's Registration Authority;
- GlobalSign CA receives notice or otherwise become aware that the 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 GlobalSign CA's jurisdiction of operation;
- Following the request for cancellation of a Certificate;
- If a Certificate has been reissued, Issuing CA may revoke the previously issued Certificate;
- Under certain licensing arrangements, Issuing CA may revoke Certificates following expiration or termination of the license agreement; and
- GlobalSign determines the continued use of the Certificate is otherwise harmful to the business of GlobalSign CA or third parties. When considering whether Certificate usage is harmful or a third party's business or reputation, Issuing CAs should consider, amongst other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force, responses to the alleged harmful use by the Subscriber;
- If Microsoft, in its sole discretion, identifies a Code Signing or EV Code Signing Certificate as either containing a deceptive name or as being used to promote malware or unwanted software, Microsoft will contact GlobalSign and request that it revoke the Certificate. GlobalSign will either revoke the Certificate within a commercially-reasonable timeframe, or request an exception from Microsoft

within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, GlobalSign will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days; or

- If Microsoft, it its sole discretion, identifies an SSL Certificate is being used to promote malware or unwanted software, Microsoft will contact GlobalSign and request that it revoke the Certificate. GlobalSign will either revoke the Certificate within a commercially-reasonable timeframe, or request an exception from Microsoft within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, GlobalSign will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days.

Revocation of a Subordinate CA Certificate shall be performed within seven (7) days under the following circumstances: -

- The Subordinate CA requests in writing to the GlobalSign entity which provided the Subordinate CA Certificate or the authority detailed in Section 1.5.2 of this CPS, that GlobalSign CA revoke the Certificate;
- The Subscriber notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains reasonable evidence that the Subordinate CA's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that the Subordinate CA has not complied with the Baseline Requirements or the applicable CP or this CPS;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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

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

4.9.2 Who Can Request Revocation

Issuing 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. Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify GlobalSign CA of a suspected reasonable cause to revoke a Certificate. Issuing CAs may also at their own discretion revoke Certificates including Certificates that are issued to other cross signed Issuing CAs.

4.9.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, Issuing CAs and RAs may provide automated mechanisms for requesting and authenticating revocation requests; for example, through an account which issued the Certificate that is requested to be revoked. RAs may also provide manual backup processes in the event that automated revocation methods are not possible.

Issuing 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 Issuing CA's CPS.

Issuing CAs and RAs shall prepare method for Subscribers, Relying Parties, Application Software Suppliers, and other third partied to submit Certificate Revocation request. Issuing CAs and RAs may or may not revoke in response to this request. See section 4.9.5 for detail of actions required for Issuing CAs and RAs for making this decision.

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. Issuing 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

Issuing CAs shall begin investigating Certificate Problem Reports within twenty-four (24) 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 Issuing CA itself, must be processed within a maximum of 30 minutes of receipt.

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

Issuing CAs and RAs shall maintains 24 x 7 ability to respond internally to a high-priority Certificate Problem Report through report abuse channel and, where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. Issuing CAs and RAs shall begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

Issuing CAs and RAs shall decide whether revocation or other action is warranted based on at least following criteria:
1. The nature of the alleged problem;
2. The number of reports received about a particular Certificate or Subscriber;
3. The entity making the complaint; and
4. Relevant legislations.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying on a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure 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). Issuing CAs may include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process.

4.9.7 CRL Issuance Frequency

All Issuing CAs must meet the requirements of the Baseline Requirements and the EV Guidelines (if applicable). In addition, Issuing CAs that operate offline shall publish a CRL every 3 months. Issuing CAs that operates online must publish CRLs at least every 24 hours.
For Subordinate CA Certificates, CRL is updated at least once every 12 months and within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than 12 months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

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

For the status of Subscriber Certificates:
Issuing CAs shall update information provided via an OCSP at least every four days. OCSP responses from this service will not exceed expiration time of ten days.

For the status of Subordinate CA Certificates:
Issuing CAs shall update information provided via an OCSP at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5 shall not respond with a "good" status for such Certificates.

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

Issuing 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 Issuing CA at their own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed Issuing 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

Certificate suspension is only allowed for Client certificates. Certificate suspension is not allowed for any other types of end entity Certificates. Certificate suspension is strictly forbidden for Server Authentication certificates.

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

Due to the nature of suspension requests and the need for efficiency, Issuing CAs and RAs may provide automated mechanisms for requesting and authenticating suspension requests; for example, through an account which issued the Certificate that is requested to be suspended. RAs may also provide manual backup processes in the event that automated suspension methods are not possible. Issuing CAs and RAs will record each request for suspension and authenticate the source, taking appropriate action to suspend the Certificate if the request is authentic and approved. Once suspended, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason code “on hold” will be included. CRLs may be published immediately or they may be published as defined within the Issuing CA’s CPS.

4.9.16 Limits on Suspension Period

There are no limits on the Certificate suspension period.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Issuing CAs shall provide a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. For Code Signing Certificates, Issuing CAs shall not remove revocation entries on CRL or OCSP until 10 years after the Expiry Date of the revoked Certificate. For other Certificate types, Issuing CAs shall not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

Issuing 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 Issuing 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 Issuing CA that offers key escrow services to Subscribers may escrow Subscriber Private Keys. Any Private Keys that are escrowed must be held in at least the same level of security as when the Key Pair was 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

Issuing 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. 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

Issuing 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

Issuing CAs shall ensure that the facilities used for Certificate lifecycle 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

Issuing 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

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

Issuing 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. 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

Issuing 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

Issuing CAs should ensure that full system backups of the Certificate issuance system are sufficient to recover from system failures and are made periodically, as defined in the Issuing CA's 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

Issuing 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:

- **Developers**: Responsible for development of CA systems.
- **Security Manager:** overall responsibility for administering the implementation of the CA's security practices, cryptographic key life cycle management functions (e.g., key component custodians);
- **Administrator:** approval of the generation, revocation and suspension of certificates;
- **System Engineer:** installation, configuration and maintenance of the CA systems, viewing and maintenance of CA system archives and audit logs;
- **Operator:** day-to-day operation of CA systems and system backup and recovery;
- **Key Manager:** cryptographic key life cycle management functions (e.g., key component custodians);

5.2.2 Number of Persons Required per Task

Issuing CAs shall state the number of persons required per task within their CPS. The goal is to guarantee the trust for all CA services (Key Pair 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, Issuing 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

Issuing 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 not permitted for any one person to serve in the following roles at the same time:

- Security officer and System Engineer or Operator;
- 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

Issuing 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. Issuing 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 Issuing CA's CPS, are documented in job descriptions. Issuing 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. Issuing 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 Issuing CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. The Issuing CA shall not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence, is such conviction affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed and results analysed, provided such checks are permitted by the jurisdiction in which the person will be employed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

Any use of information revealed by background checks by the Issuing CA shall be in compliance with applicable laws of jurisdiction where the person is employed.

5.3.3 Training Requirements

Issuing 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; and
- Disaster recovery and business continuity procedures.

Issuing CA and RA personnel shall be retrained when changes occur in Issuing CA or RA systems. Refresher training shall be conducted as required and Issuing 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 Issuing CA or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan with at least annual training on information security, and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

Issuing 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 Issuing 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

Issuing CA should make available to its personnel this CP, any corresponding CPS 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 Issuing 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.

Issuing CAs should ensure all events relating to the lifecycle 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; and
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs should be reviewed periodically 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 provide 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 individuals with authorized trusted access are able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.

The records of events must be protected in a manner to prevent alteration and detect tampering.

The records of 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, and 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 initiated 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 the Issuing CAs must determine whether to suspend Issuing 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

Issuing CAs shall perform regular vulnerability assessments covering all Issuing 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

Issuing 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 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 as well as the actual CRL.

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.

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 timestamping service is used to date the records, it must comply with the requirements defined in Section 6.8. Irrespective of timestamping 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 complies with the security requirements defined in Section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of Issuing 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 Issuing CA equipment, trusted role and other authorized persons are allowed to access the archive.

5.6 Key Changeover

Issuing CAs may periodically changeover Key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may be modified and Certificate profiles may be altered to adhere to new best practices. Private 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

Issuing 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 Issuing CA services. Issuing 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 included in the scope of the audit process as described in Section 8 to validate which operations should be first restored after a disaster and the recovery plan.
Issuing CA personnel that serve in a trusted role and operational role should be specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.

If an Issuing 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 Issuing 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 Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to the Issuing CA's disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In the event an Issuing CA Private Key is Compromised, lost, destroyed or suspected to be Compromised:

- The Issuing CA shall, after investigation of the problem, decide whether the Issuing 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; and
    - A new Issuing 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.

5.8 CA or RA Termination

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

- Stop delivering Certificates according to and referring to this CP;
- Archive all audit logs and other records prior to termination;
- Destroy all Private Keys upon termination;
- Ensure archive records are transferred to an appropriate authority such as another Issuing CA that delivers identical services; and
- 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

Issuing 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 or the ceremony, as a whole, must be videotaped/recorded. Issuing CA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

Subscriber key generation by GlobalSign is performed in a secure cryptographic device meeting FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

6.1.2 Private Key Delivery to Subscriber

Issuing CAs that create Private Keys on behalf of Subscribers may do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. The cryptographic algorithms regarding Public/Private key generation (encryption, sign, cryptographic hash, RNG or PRNG etc.) were approved by FIPS, the Public/Private key generation algorithm is also specified in FIPS 186-4.
The generated Public/Private key is encrypted with PIN code which was provided by the Subscriber. The encrypted Public/Private key will be delivered in TLS session, authenticated by the password pre-registered by an administrator of the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

Issuing 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 accordance with Section 3.2.1 of this CP.

6.1.4 CA Public Key Delivery to Relying Parties

Issuing CAs shall ensure that Public Key delivery to Relying Parties is undertaken in such a 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 by the Subscriber in the form of a chain of Certificates or via a Repository operated by the Issuing CA and referenced within the profile of the issued Certificate.

6.1.5 Key Sizes

GlobalSign CA follows NIST Special Publication 800-133 (2012) - Recommendation for Cryptographic Key Generation - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Issuing CAs and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root program, outside of the direct control of GlobalSign CA are contractually obligated to use the same best practices.
GlobalSign CA selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the Baseline Requirements and EV Guidelines: -

RSA

- 2048 bit RSA key with Secure Hash Algorithm 1 (SHA-1)
- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)
- 4096 bit RSA key with Secure Hash Algorithm 2 (SHA-384)

ECC

- 256 bit ECDSA key with Secure Hash Algorithm 2 (SHA-256)
- 384 bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
- 521 bit ECDSA key with Secure Hash Algorithm 2 (SHA-512)

6.1.6 Public Key Parameters Generation and Quality Checking

Issuing CAs shall generate Key Pairs in accordance with FIPS 186 and shall use reasonable techniques to validate the suitability of Public 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)

Issuing 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

Issuing 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. Issuing 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, through limitation to a suitable CSP (Cryptographic Service Provider) tied to a known FIPS compliant hardware platform as part of the enrollment process.

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

Issuing 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

Issuing CAs shall not escrow CA Private Keys for any reason.

6.2.4 Private Key Backup

Issuing 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

With the exception of Digital Signing Service, Issuing CAs shall not archive Private Keys and must ensurethat any temporary location where a Private Key may have existed in any memory location during the generation process is purged.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Issuing CA Private Keys must be generated, activated and stored in 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

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

6.2.8 Method of Activating Private Key

Issuing 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 accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

Issuing 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 Issuing CA's Hardware Security 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

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

Private Keys generated by GlobalSign are stored in GCC in PKCS 12 format until the Key Pairs are picked up by the Subscriber. When the Subscriber acknowledge the receipt of the Key Pair or when 30 days has passed after the key generation, the Subscriber Key Pair is automatically deleted from GCC. Subscriber Private Keys are not stored in any other systems.

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

Issuing CAs must archive Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Issuing CA Certificates and renewed Certificates shall have a maximum validity period of: -

Type	Private Key Usage	Max Validity Period
• **Root Certificates**[2]	20 years	30 years
• **TPM Root Certificates**	30 years	40 years
• **Issuing CA**	11 years	15 years
• **CA for AATL Certificates**	No stipulation	181 months
• **Trusted Root**	No stipulation	10 years
• **PersonalSign Certificates**	No stipulation	39 months
• **Noble Energy Certificates**	No stipulation	5 years
• **Code Signing Certificates**	No stipulation	39 months
• **EV Code Signing Certificates**	No stipulation	39 months
• **AATL Certificates**	No stipulation	39 months
• **DV SSL Certificates**	No stipulation	39 months

[2] *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.*

• **AlphaSSL Certificates**	No stipulation	39 months
• **OV SSL & ICPEdu Certificates**	No stipulation	39 months
• **Intranet SSL**	No stipulation	5 years
• **EV SSL Certificates**	No stipulation	27 months
• **Time Stamping Certificates**	11 years	11 years
• **NAESB Certificates**	2 years	2 years

Issuing CAs must comply with the Baseline Requirements with respect to the maximum validity period, in some cases thereby reducing the effective available Certificate term. In some cases, the maximum validity period may not be realized by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

In no event shall Issuing CAs issue an SSL/TLS Certificate with a validity period greater than 39 months whether as initial issue, re-key, reissue or otherwise.

Effective March 1, 2018, in no event shall Issuing CAs issue an SSL/TSL Certificate with a validity period greater than 825 days whether as initial issue, re-key, reissue or otherwise.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of Issuing CA activation data used to activate Issuing 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

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

6.4.3 Other Aspects of Activation Data

Issuing CA activation data must only be held by Issuing 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 Issuing CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of strong password policy;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide means for malicious code protection;
- Provide means to maintain software and firmware integrity;
- Provide domain isolation and partitioning different systems and processes; and
- Provide self-protection for the operating system.

6.5.2 Computer Security Rating

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

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for the Issuing 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 are developed in a controlled environment, and the development processes 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 are 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 installed on the equipment and are obtained from sources authorized by local policy. Issuing CA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment; and are installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

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

6.6.3 Lifecycle Security Controls

Issuing CA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware that are evaluated and certified.

6.7 Network Security Controls

Issuing CA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security 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 Timestamping

All Issuing CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping 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; and
- 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)

Issuing CAs shall issue Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

Issuing CAs shall issue 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

Issuing CAs shall issue 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

Issuing CAs shall issue Certificates with name forms compliant to RFC 5280. Within the domain of each Issuing CA, Issuer CAs shall include a unique non-sequential Certificate serial number greater than zero (0) containing at least 64 bits of output from a CSPRNG.
The content of the Certificate Issuer Distinguished Name field shall match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.5 Name Constraints

Issuing CAs may issue Subordinate CA Certificates with Name Constraints and mark as critical where necessary. In case of Name Constraints are NOT set on Subordinate CA, such CA must be subject for full audit specified in section 8.0 of this document.

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

Issuing CAs may issue Certificates with a policy qualifier and suitable text to aid Relying Parties in determining applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

Issuing 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)

Issuing 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 Issuing CAs are required to operate. Issuing CAs that are not constrained by dNSNameConstraints are audited for compliance to one or more of the following standards: -

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing
- AICPA/CICA WebTrust for Certification Authorities – SSL Baseline with Network Security

8.1 Frequency and Circumstances of Assessment

Issuing CAs are required to complete a compliance audit (where products and services offered require compliance) via a Qualified Auditor on at least an annual basis. The audit must cover the Issuing CA and its associated RA. This requirement is recursive through the hierarchy for all Issuing CAs that are not constrained by dNSNameConstraints. Constrained Issuing 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 Issuing 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 such as stipulated in section 8.0 of this document;
- 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 ($1,000,000) in coverage.

8.3 Assessor's Relationship to Assessed Entity

Issuing CAs must choose an auditor/assessor who is completely independent from the Issuing 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 Issuing CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

Issuing 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 and 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 GlobalSign Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan.

8.7 Self Audit

Issuing CA shall monitor its adherence to this Certificate Policy, Issuing CA's Certification Practice Statement and other external requirements specified in the "*Acknowledgements*" section and strictly control its service quality by performing self audits on at least a quarterly basis against randomly selected samples of at least 3 percent (6% for EV SSL Certificate and EV Code Signing Certificate) of the Certificates issued.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Issuing CAs may charge fees for Certificate issuance or renewal. Issuing 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

Issuing CAs may charge for access to any database which stores issued Certificates.

9.1.3 Revocation or Status Information Access Fees

Issuing 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 Issuing CAs Certificate status infrastructure.

9.1.4 Fees for Other Services

Issuing CAs may charge for other additional services such as timestamping.

9.1.5 Refund Policy

Issuing 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

Issuing CAs that have no name constraints imposed on their Issuing CA shall maintain Commercial General Liability insurance with policy limits of at least two million US dollars ($2,000,000) in coverage and Errors and Omissions / Professional Liability insurance with a policy limit of at least five million ($5,000,000) US dollars in coverage. The Issuing 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

Issuing 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

Issuing CAs shall protect confidential information. Issuing 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

Issuing CAs shall protect personal information in accordance with a privacy policy published on a suitable Repository along with this CP.

9.4.2 Information Treated as Private

Issuing 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 Certificate

and those who are unsuccessful and rejected. Issuing 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

Issuing CAs are responsible for securely storing private information in accordance 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 required from the Applicant to allow the use of such information. Issuing 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 Issuing CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Issuing 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

Issuing 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. Issuing 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

Issuing 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 Issuing 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.

Issuing CA represents and warrants to Certificate Beneficiaries , during the period when the Certificate is valid, Issuing CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate: -

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, Issuing CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, Issuing CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, Issuing CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, Issuing CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's

subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if Issuing CA and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if Issuing CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);
- **Status:** That Issuing CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That Issuing CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements, EV Guidelines and/or EV Code Signing Guidelines (as applicable) (see Section 4.9.1).

In addition, Issuing CA represents and warrants to Certificate Beneficiaries for NAESB Certificates that, during the period when the Certificate is valid, Issuing CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:

- Issuing CA has issued, and will manage, the Certificate in accordance with the NAESB WEQ PKI Standards.
- Issuing has complied with all requirements in the NAESB WEQ PKI Standards when identifying the Subscriber and issuing the Certificate.
- There are no misrepresentations of fact in the Certificate actually known to or reasonably knowable by Issuing CA and Issuing CA has verified information in the Certificate.
- Information provided by the Applicant for inclusion in the Certificate has been accurately transcribed to the Certificate.
- The Certificate meets the material requirements of the NAESB WEQ PKI standards.

In lieu of the warranties set forth above, Issuing CA represents and warrants to Certificate Beneficiaries for EV Certificates and EV Code Signing Certificates that, during the period when the Certificate is valid, Issuing CA has followed the Guidelines and its Certification Practice Statement in issuing and managing the Certificate and in verifying the accuracy of the information contained in the EV Certificate and/or EV Code Signing Certificate:

- **Legal Existence:** Issuing CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- **Identity:** Issuing CA has confirmed that, as of the date the Certificate was issued, the legal name of the Subject named in the Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- **Right to Use Domain Name:** For EV Certificates only, Issuing CA has taken all steps reasonably necessary to verify that, as of the date the Certificate was issued, the Subject named in the Certificate has the right to use all the Domain Name(s) listed in the Certificate;
- **Authorization for EV Certificate:** Issuing CA has taken all steps reasonably necessary to verify that the Subject named in the Certificate has authorized the issuance of the Certificate;
- **Accuracy of Information:** Issuing CA has taken all steps reasonably necessary to verify that all of the other information in the Certificate is accurate, as of the date the Certificate was issued;
- **Subscriber Agreement:** The Subject named in the Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
- **Status:** Issuing CA will follow the requirements of the EV and/or EV Code Signing Guidelines (as applicable) and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the Certificate as Valid or revoked; and
- **Revocation:** Issuing CA will follow the requirements of the EV and/or EV Code Signing Guidelines and revoke the Certificate for any of the revocation reasons specified in the EV and/or EV Code Signing Guidelines.

9.6.1.1 CA Representations and Warranties for NAESB Certificates

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

- Issued, and will manage, the Certificate in accordance with the NAESB Business Practice Standards;
- Complied with all requirements in the NAESB Business Practice 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; and
- That the Certificate meets the material requirements of the NAESB Business Practice standards.

9.6.2 RA Representations and Warranties

Issuing 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

Subscribers and/or Applicants warrant that: -

- Subscriber will provide accurate and complete information at all times to Issuing CA, both in the Certificate Request and as otherwise requested by Issuing CA in connection with issuance of a Certificate;
- Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;
- Subscriber shall review and verify the Certificate contents for accuracy;
- Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate;
- Subscriber shall respond to Issuing CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours; and
- Applicant acknowledges and accepts that Issuing CA is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if Issuing CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.3.1 North American Energy Standards Board (NAESB) Subscribers

Subscribers participating in the NAESB WEQ PKI Standard 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 WEQ PKI Standards, 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 the NAESB WEQ PKI Standards.

Each subscriber organization acknowledges their understanding of the following obligations of the NAESB WEQ PKI Standard through GlobalSign CA as follows: -

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

A. Subscriber 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. Subscriber acknowledges the industry’s endorsement of public key cryptography which utilizes Certificates to bind a person’s or computer system’s Public Key to its entity and to support symmetric encryption key exchange.

C. Subscriber has evaluated each of its selected **C**ertification **A**uthority’s CPS in light of those industry standards as identified by the Certification Authority.

Subscribers 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.

Subscribers shall also be required to comply with the following requirements:

- Protect their Private Keys from access by other parties;
- Identify, if applicable through the NAESB EIR, that they have selected GlobalSign to use as their Authorized Certification Authority;
- Execute all agreements and contracts with GlobalSign as required by GlobalSign’s CPS necessary for GlobalSign to issue Certificates to the end entity for use in securing electronic communications;
- Comply with all obligations required and stipulated by GlobalSign in this certification practices agreement, e.g., Certificate application procedures, Applicant identity proofing/verification, and Certificate management practices; and
- 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 Issuing CA’s Certificate warrants to:

- Have the technical capability to use Certificates;
- Receive notice of the Issuing CA and associated conditions for Relying Parties;
- Validate an Issuing CA’s Certificate by using Certificate status information (e.g. a CRL or OCSP) published by the issuing CA in accordance with the proper Certificate path validation procedure;
- Trust an Issuing 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 Issuing CA’s Certificate, only as it may be reasonable under the circumstances; and
- 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 Issuing 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 the NAESB WEQ PKI 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

Issuing 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 Issuing CA should be limited in accordance with any warranty policy and any limitations set forth in its CPS.

9.8.1 Exclusion of Certain Elements of Damages

Issuing CAs should make statements in their CPS to the effect that in no event (except for fraud or wilful misconduct) is the Issuing 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; and
- 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 Issuing CA's indemnification obligations must be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including any obligation to third party beneficiaries.

9.9.2 Indemnification by Subscribers

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

9.9.3 Indemnification by Relying Parties

The Issuing 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 such time as communicated otherwise by 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

Issuing 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 GlobalSign CA must be addressed to: legal@globalsign.com or by post to GlobalSign in the address provided 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

Issuing 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) complaining parties agree to notify GlobalSign of the dispute in an effort 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 complaining 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 three 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 Certificates or other products and services. The laws of Belgium also apply 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 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 GlobalSign CA, Subscribers and Relying Parties) agree to comply with 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 Entire Agreement

The Issuing 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.

9.16.3 Assignment

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

9.16.4 Severability

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

9.16.5 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 Issuing CAs that want to subscribe to the Trusted Root CA chaining service of GlobalSign must adhere to this CP and all of 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 the Trusted Root Subscriber and GlobalSign;
- Submission and publication of a CPS reviewed and acceptance by GlobalSign and/or GlobalSign auditors; and
- Submission of PKI infrastructure review by Trusted Root Subscriber and acceptance by GlobalSign and/or GlobalSign auditors.

9.17.1 CA Chaining Agreement

The CA chaining Agreement includes the following terms and conditions:

- Use of Trusted Root 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 CPS reviewed and accepted by GlobalSign;
- Compliance with this CP;
- 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 Subordinate CA Private Key management;
- No cross-signing allowed;
- Enforcement of export controls for issued Certificates in compliance 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 CPS; and
- Acceptance of Subscriber that GlobalSign might publish Subscriber CA in a GlobalSign repository.

If GlobalSign and/or GlobalSign auditors determine that the Trusted Root Subscriber has breached the CA chaining agreement GlobalSign may revoke the Subordinate CA Certificate.

9.17.2 PKI Infrastructure review

Execution of Trusted Root Subscriber Agreement is subject to review and acceptance by GlobalSign and/or GlobalSign auditors of Subscriber PKI infrastructure review.
This review documents the Subscriber CA hierarchy and its 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; and
- HSM type and serial numbers.

9.17.3 Subscriber CA implementation

GlobalSign requires a mandatory test signing of a Subscriber CA with a GlobalSign test CA. GlobalSign test CA duplicates the GlobalSign Root CA but it is identified as for testing purposes (CAT versus CA) and is not distributed to third party applications. Only after successful test signing is the 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 any changes previously reported in section. GlobalSign will instruct its Qualified Auditors, as part of its own WebTrust for CA audit, to audit annually the requirements as stated above and will also obtain from an independent third party offering web site scanning services a list of any publicly available domains to ensure compliance.