GlobalSign
Certificate Policy

Date: September 15, 2024

Version: v7.4

Table of Contents

Document History

Version	Release Date	Description
7.0	March 28, 2023	Updated naming of "PSD2" Certificates to "Open Banking" Updates for CA/B Forum ballots CSC-13 and CSC-17 Revision of OIDs Removed requirement of digitally signing this document for release Clarified “subject uniqueness” Included RA as a role in the notification and revocation process Review of audit logging and records archival sections Review of private key protection and cryptographic module engineering section Clarified revocation limitations of short-term Certificates Grammatical updates, language consistency
7.1	August 21, 2023	Updates for Baseline Requirements for S/MIME Updates for Baseline Requirements for TLS (v2.0.0) Updates to revocation reasons and status changes Review of Registration Authorities and Enterprise RAs Review of Representations and Warranties Clarified revocation limitations of short-term Certificates Grammatical updates, language consistency
7.2	November 15, 2023	Revision of key usage periods
7.3	March 29, 2024	Introduction of Mark Certificates Termination of UK eIDAS services Added overview of industry standards and regulations per product type Clarification of Certificate Problem Report procedure Improved product scoping of validation methods and re-use limitations Improved product scoping of certificate revocation process Review of key pair generation and installation section Alignment with latest ETSI standards Updates to representations and warranties Grammatical updates, language consistency
7.4	September 15, 2024	Updates to policy for processing CAA records Included references to Regulation (EU) 2024/1183 (European Digital Identity Framework) Review of audit logging and records archival sections Removed references to UK eIDAS Grammatical updates, language consistency

Acknowledgments

GlobalSign® and the GlobalSign Logo are registered trademarks of GMO GlobalSign K.K.

1.0 Introduction

This Certificate Policy (CP) applies to the products and services of GlobalSign NV/SA and affiliated entities ("GlobalSign"). Primarily, this pertains to the issuance and lifecycle management of Certificates including validity checking services. GlobalSign 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. 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.

This CP aims to comply with the requirements of:

- Browsers' root programs
- 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
- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers ("ETSI 319 401")
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements ("ETSI 319 411-1")
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates ("ETSI 319 411-2")
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps ("ETSI 319 421")
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking ("ETSI 119 495")

This CP conforms to current versions of the CA/Browser Forum Requirements:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements for TLS")
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates ("EV Guidelines")

- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing ("Baseline Requirements for Code Signing")
- CA/Browser Forum Baseline Requirements for S/MIME ("Baseline Requirements for S/MIME")

published at http://www.cabforum.org. If there is any inconsistency between this document and the CA/Browser Forum Requirements above, the CA/Browser Forum Requirements take precedence over this document.

This CP also conforms to the current version of the Minimum Security Requirements for Issuance of Mark Certificates ("MC Requirements") published at https://bimigroup.org. In the event of any inconsistency between this document and those Requirements, those requirements take precedence over this document.

This CP addresses areas of policy and practice such as, but not limited to, technical requirements, security procedures, personnel and training needs, which are required to meet industry best practices for Certificate lifecycle management. This CP applies to all Certificates issued by GlobalSign 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 applicable to 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.

The English version of this CP is the primary version. In the event of any conflict or inconsistency between the English CP and any localized or translated version, the provisions of the English version shall prevail.

1.1 Overview

This CP applies to the complete GlobalSign hierarchy of GlobalSign and all Certificates that it issues either directly through its own systems, including self-signed Root Certificates and Key Pairs. The purpose of this CP is to present GlobalSign's practices and procedures in managing Root Certificates and Issuing CAs in order to demonstrate compliance with formal industry accepted accreditations such as WebTrust.

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.

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 policies are subject to audit by authorised third parties which GlobalSign highlights on its public facing web site via a WebTrust Seal of Assurance. Additional information can be made available upon request.

1.1.1 Certificate Naming

The GlobalSign Certificates governed by this CP are:

GlobalSign Public Root CA Certificates

- GlobalSign Root CA – R1 with fingerprint EBD41040E4BB3EC742C9E381D31EF2A41A48B6685C96E7CEF3C1DF6CD4331C99
- GlobalSign Root CA – R3 with fingerprint CBB522D7B7F127AD6A0113865BDF1CD4102E7D0759AF635A7CF4720DC963C53B
- GlobalSign Root CA – R5 with fingerprint 179FBC148A3DD00FD24EA13458CC43BFA7F59C8182D783A513F6EBEC100C8924
- GlobalSign Root CA – R6 with fingerprint 2CABEAFE37D06CA22ABA7391C0033D25982952C453647349763A3AB5AD6CCF69
- GlobalSign Root CA – R46 with fingerprint 4FA3126D8D3A11D1C4855A4F807CBAD6CF919D3A5A88B03BEA2C6372D93C40C9
- GlobalSign Root CA – E46 with fingerprint CBB9C44D84B8043E1050EA31A69F514955D7BFD2E2C6B49301019AD61D9F5058

GlobalSign Public Non-TLS Root CA Certificates

- GlobalSign Client Authentication Root R45 with fingerprint 165C7E810BD37C1D57CE9849ACCD500E5CB01EEA37DC550DB07E598AAD2474A8
- GlobalSign Client Authentication Root E45 with fingerprint 8B0F0FAA2C00FE0532A8A54E7BC5FD139C1922C4F10F0B16E10FB8BE1A634964
- GlobalSign Code Signing Root R45 with fingerprint 7B9D553E1C92CB6E8803E137F4F287D4363757F5D44B37D52F9FCA22FB97DF86
- GlobalSign Code Signing Root E45 with fingerprint 26C6C5FD4928FD57A8A4C5724FDD279745869C60C338E262FFE901C31BD1DB2B
- GlobalSign Document Signing Root R45 with fingerprint 38BE6C7EEB4547D82B9287F243AF32A9DEEB5DC5C9A87A0056F938D91B456A5A
- GlobalSign Document Signing Root E45 with fingerprint F86973BDD0514735E10C1190D0345BF89C77E1C4ADBD3F65963B803FD3C9E1FF
- GlobalSign Secure Mail Root R45 with fingerprint 319AF0A7729E6F89269C131EA6A3A16FCD86389FDCAB3C47A4A675C161A3F974
- GlobalSign Secure Mail Root E45 with fingerprint 5CBF6FB81FD417EA4128CD6F8172A3C9402094F74AB2ED3A06B4405D04F30B19
- GlobalSign Timestamping Root R45 with fingerprint 2BCBBFD66282C680491C8CD7735FDBBAB7A8079B127BEC60C535976834399AF7
- GlobalSign Timestamping Root E46 with fingerprint 4774674B94B78F5CCBEF89FDDEBDABBD894A71B55576B8CC5E6876BA3EAB4538
- GlobalSign IoT Root R60 with fingerprint 36E80B78775DDA9D0BAC964AC29D5A5EC4F3684E0C74445E954A191C2939B8E0
- GlobalSign IoT Root E60 with fingerprint 43ED443C1F0CD46C9914B4272C24DC42CF6FE62B4AAB37585878A26D882AE4CB
- GlobalSign Verified Mark Root R42 with fingerprint CD122CB877C6928B9017B0F0B80DBD508196300BBD03CD7356C3BEEF524E7E0B

The Root Certificates above are Public, WebTrust-audited Certificates that are configured for non-TLS use, to cater to GlobalSign's various product offerings. GlobalSign actively promotes the inclusion of the Root Certificates above in hardware and software platforms that are capable of supporting Certificates and associated cryptographic services according to the specified GlobalSign use case and applicable hardware/software trust bits. Where possible, GlobalSign will seek to enter into a contractual agreement with platform providers to ensure effective Root Certificate life cycle management. However, GlobalSign also actively encourages platform providers at their own discretion to include GlobalSign Root Certificates without contractual obligation.

GlobalSign Non-public Root CA Certificates

- GlobalSign Non-Public Root CA – R1 with fingerprint 8D2EEFC79397F86BD4DB5B16A84144156D7EE352B57DE36B2C4FC738081DF9C9
- GlobalSign Non-Public Root CA – R2 with fingerprint 24FD17248F3B76F82AF2FD9C57D60F3EF60551508EE98DC460FD3A67866ECCEA
- GlobalSign Non-Public Root CA – R3 with fingerprint A3BB9A2462E728818A6D30548BD3950B8C8DAE1B63FC89FE66E10BB7BAB5725A
- GlobalSign Non-Public Root R43 with fingerprint D6273949002299CC84DA84984EAF3F20F4B09CC2A7B241DFD4B361A8432460EB
- GlobalSign Trusted Platform Module Root CA with fingerprint F27BF02C6E00C73D915EEB6A6A2F5FBF0C31AE0393149E6B5C31E41B113841C3
- GlobalSign Trusted Platform Module ECC Root CA with fingerprint 5A8C7B5EB888CFCE9322068E80E82B28B554FFEB7FDC9638DCB3763077401D26

GlobalSign actively promotes the inclusion of the Root Certificates above into hardware and software platforms that are capable of supporting Certificates and associated cryptographic services. Where possible, GlobalSign will seek to enter into a contractual agreement with platform providers to ensure effective Root Certificate lifecycle management. However, GlobalSign also actively encourages platform providers at their own discretion to include GlobalSign Root Certificates without contractual obligation. Roots R2 & R4 are no longer owned by GlobalSign nv/sa.

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.

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 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 makes available Certificates that can be used for non-repudiation/contentCommitment, 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 accepts comments regarding this CP addressed to the address stated in Section 1.5, *Policy Administration.*

1.1.2 Industry standards and regulations

The following industry standards and regulations apply per certificate type:

Certificate type	Applicable industry standard(s) and regulations
AATL	AATL Technical Requirements
Code Signing	Baseline Requirements for Code Signing
Qualified Certificates for electronic signatures and seals	ETSI 319 401 ETSI 319 411-1 ETSI 319 411-2 eIDAS Regulation
Qualified Certificates for electronic seals (PSD2) and Qualified Website Authentication Certificates (PSD2)	ETSI 319 401 ETSI 319 411-1 ETSI 319 411-2 ETSI 119 495 eIDAS Regulation
Qualified Website Authentication Certificates	ETSI 319 401 ETSI 319 411-1 ETSI 319 411-2 eIDAS Regulation
Qualified timestamping	ETSI 319 401 ETSI 319 421 eIDAS Regulation
S/MIME	Baseline Requirements for SMIME
TLS	Baseline Requirements for TLS
Extended Validation TLS	EV Guidelines
Mark	MC Requirements

1.2 Document Name and Identification

This document is the GlobalSign Certificate Policy.

The OID for GlobalSign NV/SA (GlobalSign) is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign (4146).

GlobalSign organizes its OID arcs for the various Certificates and documents described in this CP as follows:

Category	OID	Description
TLS	**1.3.6.1.4.1.4146.10.1**	**TLS Policies Arc**
	1.3.6.1.4.1.4146.10.1.1	Extended Validation TLS Policy
	1.3.6.1.4.1.4146.10.1.2	Organization Validation TLS Policy
	1.3.6.1.4.1.4146.10.1.3	Domain Validation TLS Policy
Authentication	**1.3.6.1.4.1.4146.10.2**	**Authentication Policies Arc**
	1.3.6.1.4.1.4146.10.2.1	Extended Validation Auth Policy
	1.3.6.1.4.1.4146.10.2.2	Organization Validation Auth Policy
	1.3.6.1.4.1.4146.10.2.3	Domain Validation Auth Policy
	1.3.6.1.4.1.4146.10.2.4	Individual Validation Auth Policy
S/MIME	**1.3.6.1.4.1.4146.10.3**	**S/MIME Policies Arc**
	1.3.6.1.4.1.4146.10.3.1	Organization Validation S/MIME Policy
	1.3.6.1.4.1.4146.10.3.2	Sponsored Validation S/MIME Policy
	1.3.6.1.4.1.4146.10.3.3	Mailbox Validation S/MIME Policy
	1.3.6.1.4.1.4146.10.3.4	Individual Validation S/MIME Policy
	1.3.6.1.4.1.4146.1.40.70	Client Certificates Policy (Email Protection)
Code Signing	**1.3.6.1.4.1.4146.10.4**	**Code Signing Policies Arc**
	1.3.6.1.4.1.4146.10.4.1	Extended Validation Code Signing Policy
	1.3.6.1.4.1.4146.10.4.2	Organization Validation Code Signing Policy
Document Signing	**1.3.6.1.4.1.4146.10.5**	**Document Signing Policies Arc**
Mark	**1.3.6.1.4.1.4146.10.6**	**Mark Arc**
	1.3.6.1.4.1.4146.10.6.1	Mark Policy

Category	OID	Description	Private Key
Qualified	**1.3.6.1.4.1.4146.1.40.36**	**eIDAS Qualified Certificates - QSCD**	
	1.3.6.1.4.1.4146.1.40.36.1	Qualified Certificates for Electronic Signatures	Private key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.36.2	Qualified Certificates for Electronic Seals	Private key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37	**eIDAS Qualified Certificates – Non QSCD**	
	1.3.6.1.4.1.4146.1.40.37.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37.3	Qualified Certificates for Electronic Seals - Open Banking	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.38	**eIDAS Qualified Certificates – Remote QSCD**	
	1.3.6.1.4.1.4146.1.40.38.1	Qualified Certificates for Electronic Signatures	Private key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.38.2	Qualified Certificates for Electronic Seals	Private key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.39	**Qualified Certificates for Authentication**	
	1.3.6.1.4.1.4146.1.40.39.1	Qualified Certificates for Authentication (Natural Persons)	
	1.3.6.1.4.1.4146.1.40.39.2	Qualified Certificates for Authentication (Legal Persons)	
	1.3.6.1.4.1.4146.1.40.39.3	Qualified Certificates for Website Authentication (QWAC)	
	1.3.6.1.4.1.4146.1.40.39.4	Qualified Certificates for Website Authentication (QWAC) – Open Banking	
	1.3.6.1.4.1.4146.1.40.41	**eIDAS Qualified Certificates – Remote Non QSCD**	
	1.3.6.1.4.1.4146.1.40.41.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed on behalf of Subscriber

Category	OID	Description
Registration Authorities	1.3.6.1.4.1.4146.1.45.1	LRA for Qualified Certificates
	1.3.6.1.4.1.4146.1.45.2	External RA for Qualified Certificates
Timestamping	1.3.6.1.4.1.4146.1.30	Timestamping Certificates Policy
	1.3.6.1.4.1.4146.1.31	Timestamping Certificates Policy – AATL
	1.3.6.1.4.1.4146.1.32	Timestamping Certificate Policy – Certificates for Qualified Timestamping (QTS) under eIDAS regulation
	1.3.6.1.4.1.4146.1.34	Hosted Timestamping Certificates Policy
	1.3.6.1.4.1.4146.1.35	Hosted Timestamping Certificates Policy – AATL
	1.3.6.1.4.1.4146.2	Policy by which the timestamping services operated by GlobalSign incorporates the time into IETF RFC 3161 responses
	1.3.6.1.4.1.4146.2.2	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 1 (SHA1)
	1.3.6.1.4.1.4146.2.3	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2)
	1.3.6.1.4.1.4146.2.3.1	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.1.1	Trusted Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.1.2	CodeSign Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.4	Policy by which the time-stamping services operated by GlobalSign incorporate the time into IETF RFC 3161 responses specifically for extended validation code signing services
	1.3.6.1.4.1.4146.2.6	JP Accredited Timestamping Tokens - AATL
	1.3.6.1.4.1.4146.2.7	JP Accredited Timestamping Tokens - non-AATL
Other Certificate Policies	1.3.6.1.4.1.4146.1.40	Non-Generic use Certificates Policy
	1.3.6.1.4.1.4146.1.40.20	Japan Certificate Authority Network (JCAN) Issuing CA Policy
	1.3.6.1.4.1.4146.1.40.30	GlobalSign AATL Certificates Policy
	1.3.6.1.4.1.4146.1.40.30.2	GlobalSign AATL Certificates Policy (Class 2)
	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
	1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy
	1.3.6.1.4.1.4146.3	GlobalSign's documents (such as Certificate Policy (CP) and Certification Practice Statement (CPS))
	1.3.6.1.4.1.4146.4	GlobalSign-specific certificate extensions Internet of Things (IoT)
	1.3.6.1.4.1.4146.5	GlobalSign Time Assessment policies
	1.3.6.1.4.1.4146.5.1	GlobalSign Japan Accredited Time Assessment Service Policy
Private hierarchy	1.3.6.1.4.1.4146.11.1	Private Hierarchy Certificate Policy Arc
	1.3.6.1.4.1.4146.11.1.1	Shared Customer Certificates Arc
	1.3.6.1.4.1.4146.11.1.1.1	IntranetSSL
	1.3.6.1.4.1.4146.11.1.1.2	IntranetS/MIME
	1.3.6.1.4.1.4146.11.1.1.3	Demo Certificates Policy – Should not be trusted as it may not contain accurate information. This is to be used for testing and integration purposes.
	1.3.6.1.4.1.4146.11.1.2	GlobalSign Internal Certificates
	1.3.6.1.4.1.4146.11.1.3	Customer Branded Certificates

Legacy OIDs

The following OIDs are marked as legacy and where applicable are being replaced with a new hierarchy indicated in the table above.

Category	OID	Description
TLS	1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy – SSL - Legacy
	1.3.6.1.4.1.4146.1.1.1	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) - Legacy
	1.3.6.1.4.1.4146.1.1.2	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) – Open Banking - Legacy
	1.3.6.1.4.1.4146.1.2	Extended Validation Certificates Policy – Code Signing - Legacy
	1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy - Legacy
	1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificates Policy – AlphaSSL - Legacy
	1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy - Legacy
	1.3.6.1.4.1.4146.1.25	IntranetSSL Validation Certificates Policy - Legacy
Qualified	1.3.6.1.4.1.4146.1.40.35	eIDAS Qualified Certificates (Generic) - Legacy
	1.3.6.1.4.1.4146.1.40.35.1	Qualified Certificates for Electronic Seals (Legal Persons with QSCD) - managed by Subscriber - Legacy
	1.3.6.1.4.1.4146.1.40.35.1.1	Qualified Certificates for Electronic Seals (Legal Persons) - Open Banking - Legacy
	1.3.6.1.4.1.4146.1.40.35.2	Qualified Certificates for Electronic Signatures (Natural Persons with QSCD) - managed by Subscriber – Legacy
	1.3.6.1.4.1.4146.40.40.1	Qualified Certificates for Website Authentication (QWAC) – Legacy
	1.3.6.1.4.1.4146.40.40.2	Qualified Certificates for Website Authentication (QWAC) – Open Banking - Legacy
Code signing	1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy (Certificates issued by GlobalSign containing 1.3.6.1.4.1.4146.1.50 are issued and managed in accordance with the Baseline Requirements for Code Signing)
Authentication	1.3.6.1.4.1.4146.1.40.60	Client Certificates Policy (Client Authentication)
Client Certificates	1.3.6.1.4.1.4146.1.40.10	Client Certificates Policy (EPKI – Enterprise PKI - Legacy)
	1.3.6.1.4.1.4146.1.40.40	Client Certificates Policy (EPKI for private CAs - Legacy)
	1.3.6.1.4.1.4146.1.40.50	Client Certificates Policy (Private Hierarchy - AEG - Legacy)
Others	1.3.6.1.4.1.4146.1.26	Test Certificate Policy –Should not be trusted as it may not contain accurate information. This is to be used for testing and integration purposes. (Legacy)
	1.3.6.1.4.1.4146.1.70	High Volume CA Policy
	1.3.6.1.4.1.4146.1.100	Internet of Things Device Certificates Policy (legacy)

Community OIDs

Certificates that comply with the applicable community requirements will include one of the following additional identifiers.

Community	OID	Description
CA/Browser Forum	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
	2.23.140.1.3	EV Code Signing Certificates Policy
	2.23.140.1.4.1	Code Signing Minimum Requirements Policy
	2.23.140.1.4.2	Code Signing Minimum Requirements Timestamping Policy
	2.23.140.1.5.1.1	S/MIME Mailbox-validated Legacy Certificate Policy
	2.23.140.1.5.1.2	S/MIME Mailbox-validated Multipurpose Certificate Policy
	2.23.140.1.5.1.3	S/MIME Mailbox-validated Strict Certificate Policy
	2.23.140.1.5.2.1	S/MIME Organization-validated Legacy Certificate Policy
	2.23.140.1.5.2.2	S/MIME Organization-validated Multipurpose Certificate Policy
	2.23.140.1.5.2.3	S/MIME Organization-validated Strict Certificate Policy
	2.23.140.1.5.3.1	S/MIME Sponsor-validated Legacy Certificate Policy
	2.23.140.1.5.3.2	S/MIME Sponsor-validated Multipurpose Certificate Policy
	2.23.140.1.5.3.3	S/MIME Sponsor-validated Strict Certificate Policy
	2.23.140.1.5.4.1	S/MIME Individual-validated Legacy Certificate Policy
	2.23.140.1.5.4.2	S/MIME Individual-validated Multipurpose Certificate Policy
	2.23.140.1.5.4.3	S/MIME Individual-validated Strict Certificate Policy
ETSI	0.4.0.194112.1.0	QCP-n: certificate policy for EU qualified Certificates issued to natural persons
	0.4.0.194112.1.1	QCP-l: certificate policy for EU qualified Certificates issued to legal persons
	0.4.0.194112.1.2	QCP-n-qscd: certificate policy for EU qualified Certificates issued to natural persons with private key related to the certified public key in a QSCD
	0.4.0.194112.1.3	QCP-l-qscd: certificate policy for EU qualified Certificates issued to legal persons with private key related to the certified public key in a QSCD
	0.4.0.194112.1.4	QCP-w: certificate for EU qualified website certificate issued to a natural or a legal person and linking the website to that person
NAESB	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

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.

The GlobalSign 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 has ultimate control over the lifecycle and management of the GlobalSign Root CA and any subsequent Subordinate CAs belonging to the hierarchy.

Henceforth and for ease of reference all CAs issuing Certificates in accordance with this CP (including GlobalSign) 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

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.

In addition to identifying and authenticating Applicants for Certificates, a Registration Authority (RA) may also initiate or pass along revocation requests for Certificates and requests for renewal and re-key of Certificates.

GlobalSign may delegate identity proofing and certificate lifecycle events to a third party, under conditions and if permitted by the applicable regulations, laws, industry standards and policies for the Certificate. Where applicable, delegation must be performed in accordance with the Industry Standards.

Third parties who enter into a contractual relationship with GlobalSign 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/B Forum. RAs may implement more restrictive vetting practices if their internal policy dictates.

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.

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 passports, eID, and drivers' licenses. Where the RA relies on Certificates issued by a third party Certification Authority, RA must review the validation practices of the third party and relying party obligations by referring to such third party's CPS.

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).

1.3.4 Relying Parties

To verify the validity of a Certificate, Relying Parties must always refer to Issuing CA's revocation information either in the form of a CRL distribution point or an OCSP responder.

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 the key usage and extended key usage values.

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
- For any application or mechanism where issues with the certificate could cause a safety risk (e.g. human or environmental risk)
- Where prohibited by law
- Qualified Certificates for Electronic Signatures should only be used by natural persons whereas Certificates for Electronic Seals should only be used by legal persons
- 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:

PACOM1 - CA Governance GlobalSign
Diestsevest 14,
3000 Leuven, Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: policy-authority@globalsign.com

1.5.2 Contact Person

General Inquiries

GlobalSign NV/SA
attn. Legal Practices,
Diestsevest 14,
3000 Leuven, Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

Certificate Problem Report

Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to:

report-abuse@globalsign.com

See Section 4.9.3.1 for the procedure for Certificate Problem Reports.

1.5.3 Person Determining CP Suitability for the Policy

PACOM1 – CA Governance 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, PACOM1 – CA Governance 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

PACOM1 – CA Governance reviews and approves any changes to the CP. Upon approval of a CP update by PACOM1 – CA Governance, 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 Industry Standards and eIDAS regulations.

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0

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.

Anti-Malware Organization: An entity that maintains information about Suspect Code and/or develops software used to prevent, detect, or remove malware.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant 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.

Authorized Certification Authority: A Certification Authority that complies with all provisions of the North American Energy Standards Board (NAESB) Business Practice Standard for Public Key Infrastructure (PKI) – WEQ-012.

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. “example.co.uk” or “example.com”). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name

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.

CA/Browser Forum Requirements: The following set of documents published by CA/Browser Forum covering requirements for issuance and management of Certificates: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates, CA/Browser Forum Network and Certificate System Security Requirements, CA/Browser Forum Baseline Requirements for Code Signing, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

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

Certificate Authority Authorization (CAA): The CAA record is used to specify which Certificate authorities are allowed to issue Certificates for a domain.

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 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 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.

Common CA Database (CCADB): A certificate repository run by Mozilla, where all publicly trusted root and issuing Certificates are listed.

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

Conformity Assessment Body: A body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides

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.

DCF77: A German longwave time signal and standard-frequency radio station.

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.

DNS CAA Email Contact: The email address defined in Appendix B.1.1. of the Baseline Requirements for TLS.

DNS TXT Record Email Contact: The email address defined in Appendix B.2.1. of the Baseline Requirements for TLS.

DNS TXT Record Phone Contact: The phone number defined in Appendix B.2.2. of the Baseline Requirements for TLS.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels 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).

eIDAS Regulation ("eIDAS"): REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

Electronic Seal: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

Electronic Signature: Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

Enterprise PKI (EPKI): A GlobalSign product for organizations to manage the full lifecycle of Microsoft Window's trusted digital IDs, Adobe Approved Trust List, including issuing, reissuing, renewing, and revoking.

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 Domain Labels of all superior nodes in the Internet Domain Name System.

Global Positioning System (GPS): A U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services.

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 type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

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.

Industry Standards: means the current versions of:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”)
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (“EV Guidelines”)
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing (“Baseline Requirements for Code Signing”)
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (“Baseline Requirements for S/MIME”)
- Minimum Security Requirements for Issuance of Mark Certificates (“MC Requirements”)
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (“ETSI 319 401”)
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (“ETSI 319 411-1”)
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (“ETSI 319 411-2”)
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (“ETSI 319 421”)

- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking ("ETSI 119 495")

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

Internationalized Domain Name (IDN): An internet domain name containing at least one language-specific script or alphabetic character which is then encoded in punycode for use in DNS which accepts only ASCII strings.

IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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.

Mark Certificate: A certificate that contains subject information and extensions specified in the MC Requirements and that has been verified and issued by a MVA in accordance with the MC Requirements but whose Mark is not a Registered Mark or a Government Mark.

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.

Network Time Protocol (NTP): A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

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.

Open Banking Certificate: A Qualified Certificate that includes Open Banking Specific Attributes.

Open Banking Specific Attributes: Attributes that are specific to Open Banking Certificates which are: which are:

- authorization number if it is issued by the NCA, or registration number recognized on national or European level or Legal Entity Identifier included in the register of credit institutions.
- role or roles of PSP;
- NCA name (NCAName) and unique identifier (NCAId).

Payment Services Directive (PSD2): European Union Directive (EU) 2015/2366 that regulates payment services and payment service providers throughout the European Union and European Economic Area.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

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.

Pseudonym: A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to an Individual's real identity.

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

Qualified Certificate: A Certificate that meets the qualification requirements defined by the eIDAS Regulation.

Qualified Certificate for Electronic Seals: A certificate for Electronic Seals, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of eIDAS Regulation.

Qualified Certificate for Electronic Signature: a certificate for Electronic Signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation.

Qualified Electronic Seals: An advanced Electronic Seal, which is created by a Qualified Electronic Seal Creation Device, and that is based on a Qualified Certificate for Electronic Seal.

Qualified Electronic Signature: An advanced Electronic Signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for Electronic Signatures.

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.

Qualified Electronic Signature/Seal Creation Device (QSCD): An electronic signature/seal creation device that meets the requirements as stipulated within Annex II of eIDAS Regulation.

Qualified Timestamping (QTS): The provisioning of timestamps that comply with Article 42 of the eIDAS Regulation.

Qualified Trust Service Provider (QTSP): a natural or a legal person who provides one or more trust services and is granted the qualified status by the supervisory body as defined within the eIDAS Regulation.

Qualified Web Authentication Certificates (QWAC): a qualified SSL Certificate that meets the requirements of article 45 of the eIDAS Regulation.

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

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

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

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

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

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.

SSL Certificate: Certificates intended to be used for authenticating servers accessible through the Internet.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. If the Subject is a device or system, it must be 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.

Supervisory Body: A body responsible for the task of supervising the qualified trust service providers established in the territory of the Member State and to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the Member State. Details are described in eIDAS Article 17.

S/MIME Certificate: Certificate intended to be used to sign, verify, encrypt, and decrypt email. Certificate with Extended Key Usage (EKU) for id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4) and the inclusion of a rfc822Name or an otherName of type id-on-SmtpUTF8Mailbox in the subjectAltName extension.

S/MIME BR Certificate: S/MIME Certificate following the Baseline Requirements for S/MIME policy.

Takeover Attack: An attack where a Signing Service or Private Key associated with a Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Industry Standards 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.

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

Validation Specialist: Someone who performs the information verification duties specified by the Baseline Requirements for TLS.

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

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 at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

Wildcard Domain Name: A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

WHOIS Lookup: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

X.400: The standard of the ITU-T (International Telecommunications Union-T) for E-mail.

X.500: The standard of the ITU-T (International Telecommunications Union-T) for Directory Services.

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
CAA	Certificate Authority Authorization
CCADB	Common CA Database
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
EPKI	Enterprise PKI
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NAESB	North American Energy Standards Board
NCA	National Competent Authority

NIST	(US Government) National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PSP	Payment service provider
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.

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 repositories for all GlobalSign public facing documentation are https://www.globalsign.com/repository and https://www.globalsign.com/en/company/corporate-policies and in the event of any inconsistency, the English version shall control.

2.2 Publication of Certificate Information

GlobalSign publishes its CP, CPS, Subscriber Agreements, and Relying Party agreements at https://www.globalsign.com/repository. The CP and CPS must include all the material required by RFC 3647, and are structured in accordance with RFC 3647.

2.3 Time or Frequency of Publication

The CA shall develop, implement, enforce, and update at least every 365 days a Certificate Policy and/or Certification Practice Statement (CP and/or CPS) that describes in detail how the CA implements the latest version of the applicable Industry Standards. The CA shall review and update its CP and/or CPS at least every 365 days, incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4 Access Controls on Repositories

The CA shall make its Repository publicly available in a read-only manner.

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. DNs (Distinguished Names) must respect name space uniqueness and must not be misleading. RFC2460 (IP version 6) or RFC791 (IP version 4) addresses may be used.

For S/MIME BR Certificates, when the subject:commonName of a Certificate issued to an Individual does not contain a Mailbox Address, it is specified as a Personal Name or Pseudonym as described in Section 7.1.4.2.2(a) of the Baseline Requirements for S/MIME. Names consisting of multiple words are permitted. Given names joined with a hyphen are considered as one single given name. Subjects with more than one given name may choose one or several of their given names in any sequence. Subjects may choose the order of their given name(s) and surname in accordance with national preference. The CA may allow common variations or abbreviations of Personal Names consistent with local practice.

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.

For S/MIME BR Certificates, Personal Names shall be a meaningful representation of the Subject's name as verified in the identifying documentation or Enterprise RA records.

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.

For S/MIME BR Certificates, the use of the subject:pseudonym attribute shall be in accordance with section 3.1.3 of the Baseline Requirements for S/MIME.

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.

3.1.4 Rules for interpreting various name forms

For S/MIME BR Certificates, interpreting various name forms shall be performed in accordance with section 3.1.4 of the Baseline Requirements for S/MIME.

3.1.5 Uniqueness of Names

No stipulation.

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

No stipulation

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 applicable Industry Standards).

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 an 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.

3.2.2.3 S/MIME BR Certificates

For S/MIME BR Certificates, the Organization identity shall be authenticated according to section 3.2.3 of the Baseline Requirements for S/MIME.

3.2.2.4 Mark Certificates

For Mark Certificates, the Organization identity shall be authenticated according to section 3.2.2 of the MC Requirements.

3.2.2.5 Qualified Certificates

GlobalSign issues three types of Qualified Certificates that include an Organization Identity:

- Qualified Certificate for Electronic Seals, which assert the identity of an Organization
- Qualified Certificates for Electronic Signatures, which assert the Individual's affiliation with an Organization.
- Qualified Website Authentication Certificates.

For all Qualified Certificates that include an organization identity, Applicants are required to indicate the organization's full legal name (including the legal form) and the address of the physical location of the Subject's place of business.

GlobalSign verifies the legal existence and the address by reference to:

- official government records provided in Qualified Government Information Sources; or
- documentation provided by or confirmation received from a government agency in the jurisdiction of the Organization's legal creation, existence or recognition; or
- records provided by a Qualified Independent Information Source.

Additionally, GlobalSign may verify the address by reference to:

- a Verified Legal Opinion or a Verified Accountant letter; or
- an attestation of the physical location signed using the Organization's valid Qualified Electronic Seal.

The information in the attestation must match the content of the Qualified Certificate.

The Full Legal Name of the Organization, doing business as names (Trade Name or Trading As Name) may also be included in the Qualified Certificate. GlobalSign will verify that the Organization has registered the use of any included doing business as name with the appropriate government agency for such filings in the jurisdiction of its Place of Business, and that such filing continues to be valid.

For Certificates that assert the Individual's affiliation with an Organization, GlobalSign will verify this affiliation by reference to:

- Confirmation provided by the Organization, obtained using a Verified Method of Communication; or
- Independent Confirmation from the Organization; or
- a Verified Legal Opinion or a Verified Accountant letter; or
- an attestation signed using the Organization's valid Qualified Electronic Seal; or
- an attestation obtained by a suitably authenticated account administrators acting in the capacity of a Local Registration Authority.

For Qualified Certificates that assert the identity of the Organization and for Qualified Website Authentication Certificates, GlobalSign will verify the identity and the authority of the Organization's authorised representative(s).

GlobalSign will verify the authority of the authorised representative(s) by reference to:

- official government records provided in Qualified Government Information Sources; or
- documentation provided by or confirmation received from a government agency in the jurisdiction of the Organization's legal creation, existence or recognition; or
- records provided by a Qualified Independent Information Source; or
- a Verified Legal Opinion or a Verified Accountant letter; or
- an attestation the signed using the Organization's valid Qualified Electronic Seal. The information in the attestation must match the content of the Qualified Certificate.

GlobalSign will verify the identity of the authorised representative in accordance with section 3.2.3.

For any Open Banking Specific Attributes, GlobalSign will validate attributes using information provided by the National Competent Authority, which includes but is not limited to national public registers, European Banking Authority registers and authenticated communication from the National Competent Authority.

If GlobalSign is notified of an email address where it can inform the NCA identified in a newly issued certificate then GlobalSign shall send to that email address information on the content of the certificate in plain text including the certificate serial number in hexadecimal, the subject distinguished name, the issuer distinguished name, the certificate validity period, as well as contact information and instructions for revocation requests and a copy of the a certificate file.

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 or domain name 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 certain identity attributes included in the request, such as his/her email address or domain name to which the Certificate relates if included in the Certificate request.

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

GlobalSign may also authenticate the Applicant's identity through one of the following methods:

1. Performing a telephone challenge/response to the Applicant using a telephone number from a reliable source; or
2. Performing a fax challenge/response to the Applicant using a fax number from a reliable source; or
3. Performing an email challenge/response to the Applicant using an email address from a reliable source; or
4. Performing a postal challenge to the Applicant using an address obtained from a reliable source; or
5. The Applicant's seal impression (in jurisdictions that permit their use to legally sign a document) is included with any application received in writing.

For AATL, the options are defined as follows. Please note that these options are also available for other Class 2 products:

1. Receiving an attestation from an appropriate notary or Trusted Third Party that they have verified the individual identity based on a Governmentally Accepted Form of ID.
2. In the case of individuals affiliated with an organization: obtaining an executed declaration of identity of the individual that includes at least one unique biometric identifier of the individual (such as a fingerprint or handwritten signature). In this executed declaration of identity, an authorized representative of the Organization mentioned in the certificate confirms having seen the individual, reviewed the individual's photo ID, and confirm that the individual's identity information in the certificate requests matches the information contained in the reviewed photo ID. GlobalSign confirms the document's authenticity directly with the authorized representative of the organization using contact information confirmed using a Qualified Independent Information Source or a Qualified Government Information Source or any other method in line with the EV Guidelines. GlobalSign confirms the authorized representative's authority to represent the Organization in line with the EV Guidelines.
3. In the case of individuals affiliated with an organization, GlobalSign may rely on attestations from the approved Local RA. Refer to 3.2.3.6 in case of a Class 2 Certificate requested through an EPKI or an MSSL profile.
4. Receiving an attestation from an organization to validate the identities of its own end customers based on a verification of a Governmentally Accepted Form of ID, while the organization maintains a secure auditable trail of these verifications.
5. Other verifications in line with the verification of individuals for Qualified Certificates.

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

If an email address is to be included in the Certificate request, GlobalSign or LRA shall verify the validity and ownership of that email address.

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 Extended Validation SSL, 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 (drivers 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.

The Applicant is also required to demonstrate control of any email address to be included in a Certificate.

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 Baseline Requirements for Code Signing.

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 S/MIME BR Certificates

For S/MIME BR Certificates, the CA shall authenticate the identity of the Individual according to section 3.2.4 of the Baseline Requirements for S/MIME.

3.2.3.5 Qualified Certificates

Verification of the Identity of Individual Subscribers must be performed according to Article 24.1 of the eIDAS Regulation.

3.2.3.6 Local Registration Authority Authentication

For Organization accounts which 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. The Organization is contractually obligated to authenticate individuals affiliated with the organization.

3.2.3.7 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 one 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

GlobalSign, 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 the Identity Proofing Process (IPP) Method described in section 2.2.2: Authentication of Subscribers of the "NAESB Accreditation Requirements for Authorized Certification Authorities."

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 or within the issued Certificate itself any exceptions that may apply to specific product types or services offered.

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.

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

For S/MIME BR Certificates, Subscriber information that has not been verified in accordance with the Baseline Requirements for S/MIME shall not be included in the Certificates.

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.
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 of the individual Applicant together with verification that the Applicant has control over the email address included if required. Additionally, verification that the Applicant Representative has the authority and approval to perform one or more of the following: to request issuance or revocation of Certificates; or to assign responsibilities to others to act in these roles. For Certificates issued through an EPKI account, the Authority of the Applicant Representative to act as an Enterprise RA 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.
S/MIME 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. Additionally, verification that the Applicant Representative has the authority and approval to perform one or more of the following: to request issuance or revocation of Certificates; or to assign responsibilities to others to act in these roles. For Certificates issued through an EPKI account, the Authority of the Applicant Representative to act as an Enterprise RA will be verified at the time of the set-up of the profile.
S/MIME BR Certificates	Validation in accordance with the Baseline Requirements for S/MIME.
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 Baseline Requirements for Code Signing.
DV/AlphaSSL Certificates	Validation of the ownership or control of the domain name is performed via one of the domain validation methods defined in Section 3.2.7.
OV SSL Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has ownership or control of the domain name 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.
Timestamping Certificates	Verification through a reliable means of communication with the organization's Applicant.
AATL	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.
Qualified Website Authentication Certificates	Verifying the authority of the contract signer, Certificate approver and the Authorised representative in accordance with the methods listed in section 3.2.2.5 together with

	verification that the Applicant has ownership or control of the domain name via the methods listed in section 3.2.7.
Qualified Certificate for Electronic Seal	Verifying the authority of the contract signer Certificate approver and the Authorised representative in accordance with the methods listed in section 3.2.2.5.
Qualified Certificate for Electronic Signature	Verification of the authenticity of the individual Applicant's request with the methods listed in section 3.2.3.5.
Mark Certificates	Verifying the authority of the contract signer and Certificate approver in accordance with the methods listed in section 3.2.2.4.

Alternative to any reliable means of communication with the organization, the authority can be confirmed using either:

- an advanced electronic signature (or higher) or seal which includes the name of the organization, its parent, subsidiary or affiliate, or
- an advanced electronic signature (or higher) of a confirmed employee or agent of the organization.

3.2.6 Criteria for Interoperation

Issuing CAs shall disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.2.7 Authentication of Domain Names

For all SSL, S/MIME and Mark Certificates, the Applicant's ownership or control of all requested FQDN(s) must be verified with methods to achieve this in accordance with the Baseline Requirements for TLS 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 to achieve an equivalent level of confidence.

3.2.8 Authentication of IP Addresses

For all SSL, S/MIME and Mark Certificates, the Applicant's ownership or control of all requested IP addresses must be verified with methods to achieve this in accordance with the Baseline Requirements for TLS 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 to achieve an equivalent level of confidence.

3.2.9 Validation of mailbox authorization or control

For all S/MIME Certificates, the Applicant's ownership of all requested email addresses must be verified with methods to achieve this in accordance with the Baseline Requirements for S/MIME section 3.2.2

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.

3.3.1 Identification and Authentication for Routine Re-key

All re-key requests must be authenticated by the Issuing CA. If at any point any information embodied in a Certificate is changed in any way, additional validation must be performed.

3.3.2 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 or RA. 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 Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Issuing CAs shall maintain their own blocklists for individuals from whom or entities from which they will not accept Certificate applications. Blocklists may be based on historic Certificates issued 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

Prior to the issuance of a Certificate, the CA shall obtain a Certificate request and an executed Subscriber Agreement and/or Terms of Use in accordance with the applicable Industry Standards.

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.

Section 6.3.2 limits the validity period of Subscriber Certificates.

The CA may reuse completed validations and/or supporting evidence in accordance with the applicable Industry Standards.

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.

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 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.

Issuing CA shall not issue publicly trusted SSL Certificates to Internal Names or Reserved IP Addresses.

Issuing CAs shall not issue publicly trusted Mark Certificates containing Internal Names.

4.2.2.1 Certification authority authorization

GlobalSign shall validate each FQDN in a publicly trusted SSL, S/MIME[1] and Mark Certificate against the domain's CAA records. GlobalSign's CAA issuer domain is "globalsign.com." If a CAA record exists that does not list globalsign.com as an authorized CA, GlobalSign shall not issue the Certificate.

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 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 or RA 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

RAs, local RA, partners/resellers, GlobalSign and other entities may be informed of the issuance if they were involved in the initial enrollment.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

---

[1] *Effective September 15, 2024*

the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate.

For Qualified Certificates where the Private Key related to the certified Public Key resides in a QSCD, Subscriber keys must be generated and stored within a recognized Qualified Signature Creation Device (QSCD).

For EV and Non-EV Code Signing Certificates, Subscriber Private Keys must be generated and protected in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+.

Where it is possible to make a backup 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 corresponding Private Keys in a conformant HSM/QSCD.

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. Relying Party must accept and act in accordance with the Relying Party Agreement 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

Certificate renewal means the issuance of a Certificate with a new validity period ending after the validity period of the old Certificate, but without changing the Subscriber or other participant's Public Key or any other information in the Certificate.

4.6.1 Circumstances for Certificate Renewal

Certificate renewal may be performed upon request of the Subscriber, an authorized representative of Subscriber or by the Issuing CA at its sole discretion.

Certificate renewal shall only be performed if the original Certificate has not been revoked.

4.6.2 Who May Request Renewal

Requests for renewal must be submitted by the Subscriber of the Certificate or their authorized representative.

4.6.3 Processing Certificate Renewal Requests

To process a renewal request, the Issuing CA must verify the request with Subscriber or their authorized representative.

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

Certificate re-key means the issuance of a new Certificate with a different Public Key, but without changing the validity period or any other information in the Certificate.

4.7.1 Circumstances for Certificate Re-Key

Certificate re-key may be performed upon request of the Subscriber, an authorized representative of Subscriber or by the Issuing CA at its sole discretion.

Certificate re-key may be requested upon compromise of the Certificate Private Key.

4.7.2 Who May Request Certification of a New Public Key

Requests for re-key must be submitted by the Subscriber of the Certificate or their authorized representative.

4.7.3 Processing Certificate Re-Keying Requests

To process a re-key request, the Issuing CA must verify the request with Subscriber or their authorized representative.

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

Certificate modification means issuance of a new Certificate due to changes in the information in the Certificate other than the Subscriber Public Key.

4.8.1 Circumstances for Certificate Modification

Certificate modification may be performed upon request of the Subscriber, an authorized representative of Subscriber or by the Issuing CA at its sole discretion.

4.8.2 Who May Request Certificate Modification

Requests for modification must be submitted by the Subscriber of the Certificate or their authorized representative.

4.8.3 Processing Certificate Modification Requests

To process a modification request, the Issuing CA must verify the request with Subscriber or their authorized representative.

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

Prior to performing a revocation, CAs must verify the authenticity of the revocation request.

The CA may revoke any Certificate at its sole discretion.

The CA shall revoke a Subscriber Certificate within twenty-four (24) hours under the following circumstances:

1. The Subscriber requests in writing (to the Issuing CA which provided the Certificate) that they wish to revoke the Certificate;
2. The Subscriber notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.
6. The Issuing CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.
7. The CA receives notice or otherwise becomes aware of unexpected termination of a Subscriber's or Subject's agreement or business functions.
8. In case of Open Banking Certificates, the CA receives an authenticated revocation request (or authenticates a revocation request) that originated from the NCA which has authorized or registered the payment service provider, and which includes a valid reason for revocation. Valid reasons for revocation include when the authorization of the PSP has been revoked or any PSP role included in the Certificate has been revoked.

The CA should revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements for algorithm type and key size of the applicable Industry Standards, as specified in Sections 6.1.5 and 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The CA receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA is made aware of any circumstance indicating that use 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);
5. The CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
7. The CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;

8. The CA is made aware that the Certificate was not issued in accordance with the applicable Industry Standards or the Issuing CA's CP and/or CPS;
9. The CA determines that any of the information appearing in the Certificate is inaccurate;
10. The CA's right to issue Certificates under the applicable CA/Browser Forum Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
11. Revocation is required by this CP and/or applicable CPS;
12. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed;
13. The technical content or 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);
14. The Issuing CA private key used in issuing the certificate is suspected to have been compromised;
15. The Issuing CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
16. The Certificate was issued in violation of the then-current version of the Mozilla Root Store Policy;
17. GlobalSign receives a Court Order of Infringement, confirms the authenticity of the Court Order of Infringement, and provides 3 business days' notice to the Subscriber that the MC will be revoked.

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

1. The Subscriber or organization administrator requests revocation of the Certificate through a customer account which controls the lifecycle of the Certificate;
2. The Subscriber requests revocation through an authenticated request to Issuing CA's support team or GlobalSign's Registration Authority;
3. The Issuing CA receives notice or otherwise becomes aware that the Subscriber has been added as a denied party or prohibited person to a blocklist, or is operating from a prohibited destination under the laws of Issuing CA's jurisdiction of operation;
4. Overdue payment of applicable fees by the Subscriber;
5. Following the request for cancellation of a Certificate;
6. If a Certificate has been re-issued, Issuing CA may revoke the previously issued Certificate;
7. Under certain licensing arrangements, Issuing CA may revoke Certificates following expiration or termination of the license agreement; and
8. The Issuing CA determines the continued use of the Certificate is otherwise harmful to the business of GlobalSign or third parties. When considering whether Certificate usage is harmful to a third party's business or reputation, GlobalSign will 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;
9. If Microsoft, in its sole discretion, identifies a certificate whose usage or attributes are determined to be contrary to the objectives of the Trusted Root Program, Microsoft will notify GlobalSign and request that it revoke the certificate. GlobalSign will either revoke the certificate or request an exception from Microsoft within 24 hours of receiving Microsoft's notice. Microsoft will review submitted material and inform GlobalSign of its final decision to 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 24 hours of the exception being denied.
10. Death of a Subscriber.

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

1. The Subordinate CA requests revocation in writing;

2. The Subscriber notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains reasonable evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements for algorithm type and key size of the applicable Industry Standards as specified in Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. 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 applicable Industry Standards or applicable CP or CPS;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. 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;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under the applicable Industry Standards expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's CP and/or CPS;
10. The technical content or 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

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the Issuing CA of 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.

Additionally, for Open Banking Certificates, revocation request can originate from the NCA which has authorized or registered the payment service provider.

4.9.3 Procedure for Revocation Request

The CA shall provide a process for Subscribers to request revocation of their own Certificates. The process shall be described in the CA's CP and/or CPS. The CA shall maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA shall provide clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA shall publicly disclose the instructions through a readily accessible online means and in Section 1.5.2 of their CPS.

4.9.3.1 Certificate Problem Reports

The CA shall describe the procedure for processing Certificate Problem Reports in its CPS.

4.9.4 Revocation Request Grace Period

For SSL and Code Signing Certificates, GlobalSign does not support a revocation request grace period.

For all other Certificates, 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.

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 maintain 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:

- The nature of the alleged problem;
- The number of reports received about a particular Certificate or Subscriber;
- The entity making the complaint; and
- Relevant legislation.

For Qualified Certificates, actual revocation status shall be published/available through all revocation mechanisms within 60 minutes after the revocation decision and will never be reverted.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying on a Certificate, Relying Parties must validate the suitability of the Certificate for the intended purpose 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. 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.

For Qualified Certificates, validation of the certificate chain shall be carried out successfully up to the Issuing CA trust anchor within the EU trusted list.

4.9.7 CRL Issuance Frequency

All Issuing CAs must meet the requirements of the applicable Industry Standards and eIDAS regulations.

For the status of Subscriber Certificates:
If the CA publishes a CRL, then the CA shall update and re-issue CRLs at least once every seven days, and the value of the nextUpdate field must not be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates:
If the Subordinate CA contains a CDP, the CA shall update and re-issue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve 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.

Issuing CAs' OCSP responses shall conforms to RFC6960 and/or RFC5019. OCSP responses shall be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

OCSP responders operated by the CA shall support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

1. OCSP responses must have a validity interval greater than or equal to eight hours.
2. OCSP responses must have a validity interval less than or equal to ten days.
3. For OCSP responses with validity intervals less than sixteen hours, then the CA shall update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA shall update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

- The CA shall update information provided via an OCSP Responder (i) at least every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a Certificate serial number that is "unused", then the responder should not respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder shall not respond with a "good" status for such requests.

The CA should monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by
    a. the Issuing CA; or
    b. a Precertificate Signing Certificate associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

If the Subscriber Certificate is for a high-traffic FQDN, Issuing CA may choose to rely on stapling, in accordance with RFC4366, to distribute its OCSP responses. In this case, Issuing CA shall ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. Issuing CA shall enforce this requirement on the Subscriber contractually through the Subscriber Agreement or Terms of Use, or by technical review measures implemented by the CA.

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 for SSL, Code Signing, timestamping, Qualified, S/MIME BR (strict profile) or Mark 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 “certificateHold” 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. Revocation entries may be removed after expiry of the Certificate to promote more efficient CRL file size management, except for Code Signing Certificates (only 10 years after expiry).

For other Certificate types, Issuing CAs shall not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

If required by Root Programs or CA/B Forum requirements, Issuing CAs may backdate revocation of Certificates with the revocationDate field, as an exception to the best practice described in RFC 5280 to use the invalidityDate field.

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. Issuing CAs shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Operational Features

No stipulation

4.11 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.

4.12 Key Escrow and Recovery

4.12.1 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.

4.12.1.1 S/MIME BR

The CA may escrow the Subscriber's Private Key as specified in the CA's CP and/or CPS.

The CA shall notify Subscribers when their Private Keys are escrowed. Escrowed Private Keys shall be stored in encrypted form. The CA shall protect escrowed Private Keys from unauthorized disclosure.

The CA shall recover Subscriber Private Keys only under the circumstances permitted within the CA's CP and/or CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation

5.0 Facility, Management, and Operational Controls

The CA shall develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process shall include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program shall include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA shall develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment,

commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan shall include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan shall also take into account then-available technology and the cost of implementing the specific measures, and shall implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

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 shall 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 shall be physically protected from unauthorized access, damage and interference, and the protections provided shall 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 life cycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee shall always accompany any unauthorized person entering a physically secured area. Physical protections shall 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 shall 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 shall ensure that the CA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

Issuing CAs shall ensure that any media used is securely handled to protect it from damage, theft and unauthorized access. Media management procedures shall be protected against obsolescence and deterioration of the media within a defined period of time. Records are required to be retained. All media shall 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 shall 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 shall 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 shall 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 shall 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 Validation Specialists 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.

GlobalSign may subscribe Certificates for GlobalSign affiliate companies, or persons identified in association with these companies (as a subject). GlobalSign affiliate companies includes GlobalSign's parent and subsidiary companies, as well and other companies that share a same parent company as GlobalSign.

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, and 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

Roles requiring a separation of duties include:

- Those performing approval of the generation, revocation, and suspension of Certificates. (Validation Specialists)
- Those performing installation, configuration, and maintenance of the CA systems. (Infra system engineer)
- Those with overall responsibility for administering the implementation of the CA’s security practices. (Security Officer)
- Those performing duties related to cryptographic key life cycle management (e.g., key component custodians). (CA activation data holders)
- Those performing CA systems development. (Developers)

- Those performing CA systems auditing (Infra Operator, Auditor)

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, Issuing CA shall verify the identity and trustworthiness of such person.

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.

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

The CA shall provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's CP and/or CPS), common threats to the information verification process (including phishing and other social engineering tactics), and the Industry Standards.

The CA shall maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

The CA shall document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA shall require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Industry Standards.

5.3.4 Retraining Frequency and Requirements

All personnel in Trusted Roles shall maintain skill levels consistent with GlobalSign's training and performance programs.

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

The CA shall verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

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

Issuing CA and each Delegated Third Party shall record events related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems. Issuing CA and each Delegated Third Party shall record events related to their actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. Issuing CA shall make these records available to its Qualified Auditor.

Issuing CA shall record at least the following events:

1. CA certificate and key lifecycle events, including:

    i. Key generation, backup, storage, recovery, archival, and destruction;
    ii. Certificate requests, renewal, and re-key requests, and revocation;
    iii. Approval and rejection of certificate requests;
    iv. Cryptographic device lifecycle management events;
    v. Generation of Certificate Revocation Lists;
    vi. Signing of OCSP Responses; and
    vii. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. Subscriber Certificate lifecycle management events, including:

    i. Certificate requests, renewal, and re-key requests, and revocation;
    ii. All verification activities stipulated in this Certificate Policy;
    iii. Approval and rejection of certificate requests;
    iv. Issuance of Certificates;
    v. Generation of Certificate Revocation Lists; and
    vi. Signing of OCSP Responses.

3. Security events, including:

    i. Successful and unsuccessful PKI system access attempts;
    ii. PKI and security system actions performed;
    iii. Security profile changes;
    iv. Installation, update and removal of software on a Certificate System;
    v. System crashes, hardware failures, and other anomalies;
    vi. Firewall and router activities; and
    vii. Entries to and exits from the CA facility.

4. Timestamp Authorities shall log the following Timestamp Authority information:
    I. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,

II. History of the timestamp server configuration,
III. Any attempt to delete or modify timestamp logs,
IV. Security events, including:
    a. Successful and unsuccessful Timestamp Authority access attempts;
    b. Timestamp Authority server actions performed;
    c. Security profile changes;
    d. System crashes and other anomalies; and
    e. Firewall and router activities;
V. Revocation and Destruction of a timestamp certificate,
VI. Major changes to the timestamp server's time, and
VII. System startup and shutdown.

Log records must include the following elements:

1. Date and time of event;
2. Identity of the person making the journal record; and
3. Description of the event.

5.4.2 Frequency of Processing Log

No stipulation.

5.4.3 Retention Period for Audit Log

Issuing CA and each Delegated Third Party shall retain, for at least two (2) years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
    i. the destruction of the CA Private Key; or
    ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate Private Key (as set forth in Section 6.3.2);
4. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

For Qualified Certificates, the retention period is at least seven (7) years after the event occurs.

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 trusted roles can perform operations 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 must be backed-up in a secure location (for example, a fire proof safe), under the control of a trusted role, and separated from their component source generation. Audit log backup should be protected to the same degree as the originals.

5.4.6 Audit Collection System

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.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Issuing CA shall perform annual risk assessments that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Issuing CA has in place to counter such threats.

Issuing CA shall also perform regular vulnerability assessment and penetration testing covering all CA assets related to Certificate issuance, products and services. Assessments 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 CA and each Delegated Third Party shall archive all audit logs (as set forth in Section 5.4.1).

Additionally, Issuing CA and each Delegated Third Party shall archive:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1) shall be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, the Issuing CA and each Delegated Third Party shall retain, for at least two (2) years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
    1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
    2. the expiration of the Subscriber Certificates relying upon such records and documentation.

For Qualified Certificates, the retention period is at least seven (7) years after the event occurs.

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 for which they are required to be held. Archive protections should ensure that only trusted roles can perform 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 Timestamping 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

No stipulation.

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 Issuing CA 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

When it is necessary to terminate an Issuing CA or RA activities, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing CA and/or Registration Authority Agreements. Issuing CAs must specify the procedures they will follow when terminating all or a portion of their Digital Certificate issuance and management operations. The procedures must, at a minimum:

- ensure that any disruption caused by the termination of an Issuing CA is minimised as much as possible;
- ensure that archived records of the Issuing CA are retained;
- ensure that prompt notification of termination is provided to Subscribers, Authorised Relying Parties, Application Software Providers, and other relevant stakeholders in GlobalSign certificate lifecycles;
- ensure Certificate status information services are provided and maintained for the applicable period after termination, including, if applicable, transferring Certificate status information services to another GMO Internet Group entity;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained;
- notify all auditors including the eIDAS Conformity Assessment Body; and
- notify the Belgian eIDAS supervisory body (FPS Economy, SMEs, Self-employed and Energy - Quality and Safety)
- notify other relevant Government and Certification bodies under applicable laws and related regulations

5.8.1 Successor Issuing Certification Authority

To the extent that it is practical and reasonable, the successor Issuing CA should assume the same rights, obligations, and duties as the terminating Issuing CA.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

For CA Key Pairs for a public Root Certificate, GlobalSign shall perform the following:

1. prepare and follow a Key Generation Script;
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process; and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For CA Key Pairs used for public Root or Subordinate CA Certificates, Issuing CA shall also perform the following:

1. prepare and follow a Key Generation Script;
2. generate the CA Key Pair in a physically secured environment as described in this CP/CPS;
3. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;

4. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CP/CPS;
5. log its CA Key Pair generation activities; and
6. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

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.

Issuing CA shall also reject a certificate request if it has a known weak Private Key.

6.1.1.2 Subscriber Key Pair Generation

For Subscriber keys generated by issuing CA, Key generation must be performed in a secure cryptographic device that meets FIPS 140-2 (or equivalent) using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6. Where applicable, Subscriber keys must be generated in accordance with the Industry Standards and eIDAS regulations.

Keys used for Code Signing Certificates must be generated on a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+.

For Qualified Certificates where the Private Key related to the certified Public Key resides in a QSCD, Issuing CA systems must ensure Subscriber keys are generated and stored within a recognized Qualified Signature Creation Device (QSCD). Issuing CAs shall monitor QSCD certification status and apply appropriate measures, including revocation, if the certification status of a QSCD changes.

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.

Where applicable, the CA shall perform private key delivery to Subscriber in accordance with section 6.1.2 of the applicable Industry Standards.

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.

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 follows NIST Special Publication 800-133 Revision 2 (2020) - 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.

GlobalSign 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 Industry Standards:

Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048[2]	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

Subordinate Certificates

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1[3], SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

Subscriber Certificates

Digest algorithm	SHA-1[4], SHA-256, SHA-384 or SHA- 512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
RSASSA-PSS[5]	

As of July 1, 2017, the minimum key size for new Root CA Certificates which issue Subordinate CAs for AATL is RSA 3072-bit or ECC NIST P-384.
As of January 1, 2021, the minimum key size for new Root and Subordinate CA Certificates which issue Code Signing and Timestamping Certificates is RSA 3072-bit or ECC NIST P-256
As of June 1, 2021, the minimum key size for new Code Signing and Timestamping Subscriber Certificates for CodeSign is RSA 3072-bit or ECC NIST P-256.

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. Where applicable, key pair generation and quality checking must be generated in accordance with the Industry Standards.

---

[2] *RSA key modulus size in bits must be divisible by 8. A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits may still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.*

[3] *SHA-1 may be used for IntranetSSL Subordinate CA Certificates, but they are not chained to publicly trusted roots.*

[4] *SHA-1 may be used for IntranetSSL Subscriber CA Certificates, but they are not chained to publicly trusted roots.*

[5] [8] *RSASSA-PSS may be used with RSA keys for PersonalSign Certificates in accordance with the criteria defined in Section 7.1.3.*[5] *RSASSA-PSS may be used with RSA keys for PersonalSign Certificates in accordance with the criteria defined in Section 7.1.3.*

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).

Private Keys corresponding to Root Certificates shall not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Issuing CAs shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. Issuing CAs shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

Issuing CAs shall protect its CA Private Key in a system or device that has been validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

Issuing CAs that require Subscribers to use specific systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection.

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 CA Private Keys under the same multi-person control as the original Private Key.

6.2.5 Private Key Archival

Issuing CAs shall not archive Private Keys and must ensure that any temporary location where a Private Key may have existed in any memory location during the generation process is purged.

For Subordinate CAs issuing Publicly-Trusted Certificates, Parties other than the Subordinate CA shall not archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

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.

If Issuing CA becomes aware that a CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the CA, then Issuing CA shall revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

Issuing CAs shall store Private Keys on a device meeting the requirements of Section 6.2.1.

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 shall only be used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, its Private Key must be 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 the HSM in such a manner that no information can be used to deduce any part of the Private Key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Issuing CAs must archive Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificates shall have a maximum validity period of:

Type	Key Pair Usage Period	Max Validity Period
Root Certificates[6]	No stipulation	25 years
TPM Root Certificates	30 years	41 years
Publicly Trusted Sub-CAs/Issuer CAs	No stipulation	18 years
PersonalSign Certificates	No stipulation	39 months
Code Signing Certificates	No stipulation	39 months
EV Code Signing Certificates	No stipulation	39 months
S/MIME BR strict and multipurpose Certificates	No stipulation	825 days
S/MIME BR legacy Certificates	No stipulation	1185 days
AATL End Entity Certificates	No stipulation	39 months
Qualified Certificate for Electronic Signatures and Seals	No stipulation	39 months
DV SSL Certificates	No stipulation	398 days
AlphaSSL Certificates	No stipulation	398 days
OV SSL Certificates	No stipulation	398 days
EV SSL Certificates	No stipulation	398 days
Qualified Website Authentication Certificates	No stipulation	398 days
Intranet SSL	No stipulation	5 years
Timestamping Certificates	15 months	11 years
NAESB Certificates	2 years	2 years
Private Key Archival\Key Recovery Agent Certificates	No stipulation	5 years

The Key Pair usage period can be up to the Certificate Validity Period.

Certificates signed by a specific CA must expire before or at the end of that CA Certificate Validity period.

[6] *2048-bit keys generated prior to 2003 using RSA may be used for the maximum period allowed in the applicable root stores.*

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day. For this reason, Subscriber Certificates should not be issued for the maximum permissible time by default, in order to account for such adjustments.

Issuing CAs must comply with the Industry Standards 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 Industry Standards 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.

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.

For accounts capable of directly causing certificate issuance, Issuing CA shall enforce multifactor authentication.

6.5.2 Computer Security Rating

No Stipulation

6.6 Life Cycle 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 Life Cycle 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.

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

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

The CA shall meet the technical requirements set forth in Section 2.2, Section 6.1.5, and Section 6.1.6.

CAs shall generate non-sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Number(s)

Certificates shall be of type X.509 v3.

7.1.2 Certificate Content and Extensions

CAs shall follow RFC 5280 and the following Industry Standards:

Certificate type	Source	Section
TLS	Baseline Requirements for TLS	7.1.2
EV TLS	EV Guidelines	9
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	7.1.2
S/MIME BR	Baseline Requirements for S/MIME	7.1.2
Mark	MC Requirements	7.1.2

Exceptions may be documented in this policy or the certifications practice statement implementing this policy.

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}
SHA384WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
SHA512WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

ECDSAWithSHA256 {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}
RSASSA-PSS {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)}

*Not used for signing publicly trusted end entity Certificates

Issuing CAs shall use signature algorithms and encodings in line with the applicable CA/Browser Forum Requirements section 7.1.3.

7.1.4 Name Forms

Issuing CAs shall issue Certificates with name forms compliant to RFC 5280 and section 7.1.4 the applicable CA/Browser Forum Requirements.

7.1.5 Name Constraints

CAs shall follow section 7.1.5 of the applicable CA/Browser Forum Requirements.

7.1.6 Certificate Policy Object Identifier

CAs shall apply the following requirements:

Certificate type	Source	Section
TLS	Baseline Requirements for TLS	7.1.6
EV TLS	EV Guidelines	9.3.2

Code Signing and EV Code Signing	Baseline Requirements for Code Signing	7.1.6
S/MIME BR	Baseline Requirements for S/MIME	7.1.6
Mark	MC Requirements	7.1.6

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.1.10 Special Provisions for Qualified Certificates

CAs issuing Qualified Certificates shall follow the applicable certificate profile requirements of ETSI EN 319 412 and ETSI TS 119 495.

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

CAs shall follow section 7.2.2 of the applicable CA/Browser Forum Requirements.

7.3 OCSP Profile

CAs shall follow section 7.3 of the applicable CA/Browser Forum Requirements.

Issuer CAs shall operate an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 or RFC 5019.

7.3.1 Version Number(s)

No stipulation

7.3.2 OCSP Extensions

No stipulation

8.0 Compliance Audit and Other Assessments

The CA shall at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with the applicable Requirements for the Certificate type;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1 Frequency and Circumstances of Assessment

CAs shall follow section 8.1 of the applicable CA/Browser Forum Requirements and the applicable requirements of the eIDAS regulations.

8.2 Identity/Qualifications of Assessor

The CA's audit 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:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
3. 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;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403 or ETSI EN 319 403-1;
5. (For audits conducted in accordance with the WebTrust standard) licensed for WebTrust by CPA Canada;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

For eIDAS, the audit shall be performed by a conformity assessment body accredited by a European Union member state national accreditation body on the basis of EN ISO/IEC 17065 as profiled by ETSI EN 319 403 and in particular against the requirements defined in the eIDAS Regulation (EU) No 910/2014.

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.

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

CAs shall follow section 8.6 of the applicable CA/Browser Forum Requirements.

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. The results could also be made available to any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement. Copies of GlobalSign's WebTrust for CAs audit reports can be found at: https://www.globalsign.com/en/repository/.

8.7 Self-Audit

CAs shall follow section 8.7 of the applicable CA/Browser Forum Requirements.

The 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.

8.8 Review of delegated parties

Except for Delegated Third Parties, Enterprise RAs, and Technically Constrained Subordinate CAs that undergo an annual audit that meets the criteria specified in Section 8.4, the CA shall ensure the practices and procedures of delegated parties are in compliance with the applicable CA/Browser Forum Requirements and the relevant CP and/or CPS. The CA shall document the obligations of delegated parties and perform monitoring on at least an annual basis of the delegated parties' adherence with those obligations.

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

No stipulation.

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

The CA shall publish a Privacy Policy that provides information on the CA's data protection practices. The Privacy Policy should include information on how the CA collects, uses, shares, store, and deletes or retains data, as well as contact information for the exercise of privacy rights.

9.4.2 Information Treated as Private

The CA or RA shall treat all personal information about an Individual that is not publicly available in the contents of a Certificate as private information. This includes information that links a Pseudonym to the real identity of the Subject Individual.

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

The CA or RA shall protect private information using appropriate safeguards and a reasonable degree of care. The CA or RA shall require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.5 Notice and Consent to Use Private Information

The CA or RA shall provide appropriate notices to, and receive the necessary consent, from Subject Individuals before using private information for any purpose other than providing services related to the issuance and management of Certificates. The CA or RA shall require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA may disclose private information where required to do so by law or regulation, without notice to Applicants or Subscribers.

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

By issuing a Certificate, the CA makes the warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root CA Certificate in software distributed by such Application Software Supplier; and

3. All Relying Parties who reasonably rely on a Valid Certificate.

The 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:

The Certificate Warranties shall specifically include, but are not limited to, the contents of the following Industry Standards:

Certificate type	Source	Section
TLS	Baseline Requirements for TLS	9.6.1
EV TLS	EV Guidelines	7.1
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	9.6.1
S/MIME BR	Baseline Requirements for S/MIME	9.6.1
Mark	MC Requirements	9.6.1

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 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

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

9.6.3 Subscriber Representations and Warranties

The CA shall require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA shall obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's acknowledgement of the Terms of Use.

The CA shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. The CA may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use must contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the obligations and warranties of the following Industry Standards:

Certificate type	Source	Section
TLS	Baseline Requirements for TLS	9.6.3
EV TLS	EV Guidelines	7.2
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	9.6.3
S/MIME BR	Baseline Requirements for S/MIME	9.6.3
Mark	MC Requirements	9.6.3

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 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 as follows:

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

- 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/contentCommitment: A party cannot deny having engaged in the transaction or having sent the electronic message.
- 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.
- Subscriber has evaluated each of its selected Certification Authority'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 certificate policy 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

No stipulation.

9.6.5 Representations and Warranties of Other Participants

For Code Signing and EV Code Signing Certificates, The CA must contractually obligate each Signing Service to inform the CA if the Signing Service becomes aware (by whatever means) that the Signing Service has signed Suspect Code. The CA must require the Signing Service to request revocation of the affected Certificate and provide immediate notice to the CA if the Signing Service's private key, or private key activation data, is compromised or believed to be compromised. The CA must revoke the affected Certificate upon request by the Signing Service or if the CA determines the Signing Service failed to notify the CA within 24 hours after identifying a private key compromise.

Signing Services must obtain the Subscriber's commitment to:

1. Use such signing services solely for authorized purposes that comply with the Subscriber Agreement/Terms of Use, the applicable CA/Brower Forum Requirements, and all applicable laws,
2. Not knowingly submit software for Code Signature that contains Suspect Code, and
3. Inform the Signing Service if it is discovered (by whatever means) that Code submitted to the Signing Service for Code Signature contained Suspect Code

9.7 Disclaimers of Warranties

Issuing CAs shall 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

For delegated tasks, the CA and any Delegated Third Party may allocate liability between themselves contractually as they determine, but the CA shall remain fully responsible for the performance of all parties in accordance with the applicable Requirements, as if the tasks had not been delegated.

If the CA has issued and managed the Certificate in compliance with the applicable Requirements and its CP and/or CPS, the CA may disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's CP and/or CPS.

If the CA has not issued or managed the Certificate in compliance with the applicable Requirements and its CP and/or CPS, the CA may seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with the applicable Requirements or its CP and/or CPS, then the CA shall include the limitations on liability in the CA's CP and/or CPS.

The CA shall follow the limitations of liability of the following Industry Standards:

Certificate type	Source	Section
TLS	Baseline Requirements for TLS	9.8
EV TLS	EV Guidelines	18
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	9.8
S/MIME BR	Baseline Requirements for S/MIME	9.8
Mark	MC Requirements	9.8

The total liability of the CA shall be limited in accordance with any warranty policy and any limitations set forth in its CPS.

9.9 Indemnities

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have agreed to distribute the Root CA Certificate do not assume any obligation or potential liability of the CA under the applicable CA/Brower Forum Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

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 document its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3 Indemnification by Relying Parties

The Issuing CA shall document 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 on its web site or Repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Changes become effective immediately upon publication.

9.10.3 Effect of Termination and Survival

Issuing CAs shall 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 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 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

This CP is reviewed at least every 365 days and may be reviewed more frequently. All changes are reviewed and approved by the GlobalSign Policy Authority before insertion.

Changes to this CP are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

Issuing CAs shall 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 Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) 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.

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, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Belgium.

9.16 Miscellaneous Provisions

9.16.1 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.

9.16.2 Assignment

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

9.16.3 Severability

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

Each and every provision of this CP that provides for a limitation of liability, is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 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

9.16.5 Force Majeure

GlobalSign shall not be liable for any losses, costs, expenses, liabilities, damages, or claims arising out of or related to delays in performance or from failure to perform its obligations if such failure or delay is due to circumstances beyond GlobalSign's reasonable control, including without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike or other, interruption of or delay in transportation, unavailability of, interruption or delay in telecommunications or third party services.

9.17 Other Provisions

No stipulation.