GlobalSign Combined Certificate Policy and Certification Practice Statement

Generic

June 15, 2026

Version 1.1

Table of Contents

Document History

Version	Release Date	Description
1.0	March 31, 2026	Initial release.
1.1	June 15, 2026	Updates for Chrome Root Program Policy, Version 1.8. Indicating adherence to the Chrome and CCADB policy and submission of TLS pre-certificates to public CT logs. Clarified validation of Certificate Subject fields.

Acknowledgments

1. Introduction

This combined Certificate Policy and Certification Practice Statement (CP/CPS), Generic, applies to the products and services of GlobalSign NV/SA and Affiliated entities (“GlobalSign”).

It covers the issuance and lifecycle management of Certificates, including Certificate status validation services.

The scope of Certificates covered by this document is defined in Overview. eIDAS Certificates for Electronic Signatures, seals and timestamping are governed by a separate CPS.

This CPS 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 at https://www.globalsign.com/repository. (*Alternative language versions may be available to aid Relying Parties and Subscribers in their understanding of this document; however, in the event of any inconsistency, the English language version shall control.)*

A CPS describes the "procedures under which a Digital Certificate is issued to a particular community and/or class of application with common security requirements.” This CPS 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 document according to the structure of RFC 3647, the topic may not necessarily apply to services of GlobalSign. These sections state ‘No stipulation.' Additional information is presented in subsections of the standard structure where necessary. 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 CPS 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
- 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 TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking (“ETSI 119 495”)

GlobalSign adheres and conforms to the latest published version of the Chrome Root Program Policy, CCADB Policy and 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 the Issuance and Management of Publicly-Trusted S/MIME Certificates (“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.

GlobalSign also conforms to the current version of the Minimum Security Requirements for Issuance of Mark Certificates 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 CPS addresses the technical, procedural and personnel policies and practices of GlobalSign during the complete lifecycle of Certificates issued by GlobalSign. This CPS addresses the requirements of the CA that issues Certificates of various types. The chaining to any particular Root CA may vary depending on the choice of intermediate Certificate and Cross Certificate used or provided by a platform or client.

This CPS 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 document.

For Subscribers, this document becomes effective and binding by accepting a Subscriber Agreement or Terms of Use. For Relying Parties, this document becomes binding by relying upon a Certificate issued under this document. In addition, Subscribers are required by the Subscriber Agreement to inform their Relying Parties that the CPS is itself binding upon those Relying Parties.

All Subscribers/Mark Asserting Entities, Consuming Entities, and Relying Parties are bound by the MC Terms in Appendix D of the MC Requirements.

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

1.1. Overview

This Generic CPS applies to the hierarchy of Certificates issued by GlobalSign. This excludes eIDAS Certificates for Electronic Signatures, seals and timestamping, identified by Issuing CAs with "Qualified" or "Itsme Sign" in the Common Name.

The purpose of this document is to present the GlobalSign practices and procedures in managing Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to GlobalSign's internal and industry requirements pursuant to the standards set out above.

This CPS aims to document GlobalSign's delivery of certification services and management of the Certificate lifecycle of any issued Subordinate CA, client, server, and other purpose end entity Certificates.

The Certificate types addressed in this document are the following:

Certificate Type	Description
PersonalSign 1	A personal Certificate of low assurance
PersonalSign 2	A personal Certificate of medium assurance
PersonalSign 2 Pro	A personal Certificate of medium assurance with reference to professional context
PersonalSign 2 Pro DepartmentSign	A machine, device, department, or role Certificate of medium assurance with reference to professional context
PersonalSign 3 Pro	A personal authentication Certificate of high assurance with reference to professional context
PersonalSign Partners	A private Certification Authority created as a trust anchor issuing PersonalSign 2 Pro or PersonalSign 2 Pro DepartmentSign
IntranetSSL	A Certificate to authenticate web servers which does not chain to a Publicly-Trusted GlobalSign Root
DomainSSL	A Certificate to authenticate web servers
AlphaSSL	A Certificate to authenticate web servers
OrganizationSSL	A Certificate to authenticate web servers
Extended Validation SSL	A Certificate to authenticate web servers
GlobalSign Timestamping	A Certificate to authenticate time sources
AATL	A Certificate of medium hardware assurance for use with Adobe AATL and Microsoft Office documents
Code Signingfootnote	A Certificate to authenticate data objects
Extended Validation Code Signing	A Certificate to authenticate data objects
North American Energy Standard Board (NAESB) Authorized CA Certificates	A personal, role, server, or device Certificate of either rudimentary, basic, or medium, with reference to professional context authorized by an Authorized Certification Authority

Certificate Type	Description
Qualified Web Authentication Certificates	eIDAS compliant Qualified Certificates for web authentication (SSL)
S/MIME	A Certificate to sign, verify, encrypt, and decrypt email.
Mark Certificate	Certificates intended for asserting a cryptographically verifiable and auditable binding between an identity, a logo, and a domain.

GlobalSign Certificates:

- Can be used for Electronic Signatures in order to replace handwritten signatures where transacting parties choose;
- Can be used to authenticate web resources, such as servers and other devices;
- Can be used to digitally sign code, documents, and other data objects; or
- Can be used for encryption of data.

This CPS identifies the roles, responsibilities and practices of all entities involved in the lifecycle, use, reliance upon and management of GlobalSign Certificates. The provisions of this document apply to practices, level of services, responsibilities, and liability bind all parties involved, including GlobalSign, GlobalSign RA, Subscribers and Relying Parties. Certain provisions might also apply to other entities such as the certification service provider, application provider, etc.

A GlobalSign Certificate Policy (CP) complements this document. The purpose of the GlobalSign CP is to state the *"what is to be adhered to"* and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services.

This CPS states *"how the Certification Authority adheres to the Certificate Policy."* In doing so, this document features a greater amount of detail and provides the end user with an overview of the processes, procedures, and conditions that GlobalSign uses in creating and maintaining the Certificates that it manages. In addition to the CP and CPS, GlobalSign maintains additional documented polices addressing 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 warranties offered by GlobalSign;
- The GlobalSign Privacy Policy on the protection of personal data; and
- The GlobalSign Certificate Policy that addresses the trust objectives for the GlobalSign Root Certificates.

A Subscriber or Relying Party of a GlobalSign Issuing CA Certificate must refer to this document in order to establish trust in a Certificate issued by GlobalSign as well as for information about the practices of GlobalSign. It is also essential to establish the trustworthiness of the entire Certificate chain of the hierarchy. This includes the Root CA Certificate as well as any operational Certificates. This can be established based on the assertions within this document. For Qualified Certificates, validation of the Certificate chain must be carried out successfully up to the GlobalSign trust anchor within the EU trusted list.

1.1.1. Certificate Naming

The GlobalSign Root CA Certificates governed by this document 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 actively promotes the inclusion of the Root Certificates above in 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 life cycle management. However, GlobalSign also actively encourages platform providers at their own discretion to include GlobalSign CA Root Certificates without contractual obligation. GlobalSign Root CA R2 & GlobalSign Root CA R4 are no longer owned by GlobalSign.

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

1.1.1.1. Public Disclosure of Subordinate Issuing CA Certificates

Browser root programs require that all Subordinate CAs that are not technically constrained (using Name Constraints and Extended Key Usage Constraints) are publicly disclosed. All “Active” Subordinate CA Certificates which chain directly or transiently to any Public Root Certificate are listed in the Common CA Database (CCADB). Retired CA Certificates that have not been revoked are reported on semi-annually to root programs via bugs or e-mails as required by the applicable root program. Revoked Subordinate CA Certificates are also reported in the same manner, either shortly after revocation if routine or immediately after for a security concern.

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, GlobalSign 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 the Subscriber as well as aspects of Certificate management such as the issuance, revocation, and expiration of the Certificate. By means of this procedure to issue Certificates, 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. 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 in which Certificates are used.

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 Website Authentication Certificates	ETSI 319 401 ETSI 319 411-1 ETSI 319 411-2 ETSI 119 495 (PSD2) eIDAS Regulation
S/MIME	Baseline Requirements for S/MIME
TLS	Baseline Requirements for TLS
Extended Validation TLS	EV Guidelines
Mark	MC Requirements

1.2. Document Name and Identification

This document is the GlobalSign Certification Practice Statement.

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 document 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	**1.3.6.1.4.1.4146.1.40.39**	**Qualified Certificates for Website Authentication**	
	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	

Category	OID	Description
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
	1.3.6.1.4.1.4146.1.34	Hosted Timestamping Certificates Policy
	1.3.6.1.4.1.4146.1.35	Hosted Timestamping Certificates Policy – 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.

Category	OID	Description
	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	1.3.6.1.4.1.4146.40.40.1	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
	2.23.140.1.5.1.2	S/MIME Mailbox-validated Multipurpose Certificate Policy
	2.23.140.1.5.1.3	S/MIME Mailbox-validated Strict Certificate Policy
	2.23.140.1.5.2.2	S/MIME Organization-validated Multipurpose Certificate Policy
	2.23.140.1.5.2.3	S/MIME Organization-validated Strict Certificate Policy
	2.23.140.1.5.3.2	S/MIME Sponsor-validated Multipurpose Certificate Policy
	2.23.140.1.5.3.3	S/MIME Sponsor-validated Strict Certificate Policy
	2.23.140.1.5.4.2	S/MIME Individual-validated Multipurpose Certificate Policy
	2.23.140.1.5.4.3	S/MIME Individual-validated Strict Certificate Policy
ETSI	0.4.0.194112.1.4	QEVCP-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
AuthIndicators Working Group	1.3.6.1.4.1.53087.1.1	Mark Certificate General Policy Identifier

1.3. PKI Participants

1.3.1. Certification Authorities

GlobalSign is a Certification Authority that issues Certificates in accordance with this document. As a Certification

Authority, GlobalSign performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. GlobalSign also provides Certificate status information 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 referred to as *"Issuing Authority"* or *"GlobalSign"* to denote the purpose of issuing Certificates at the request of a Registration Authority (RA) from a subordinate Issuing CA.

The GlobalSign PACOM1 - CA Governance Policy Authority is responsible for maintaining this document 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 Issuing CAs belonging to the hierarchy.

GlobalSign is also a Timestamping Authority (TSA) and provides proof of existence of data at a particular point in time. GlobalSign may outsource specific TSA services as necessary to allow for additional independent verification of time related functions.

GlobalSign ensures the availability of all services pertaining to the management of Certificates under the GlobalSign Roots, including without limitation the issuance, revocation, and status verification of a Certificate, as they may become available or required in specific applications. GlobalSign also manages a core online registration system and a number of APIs for all Certificate types issued under GlobalSign Subordinate/Issuing CAs.

Some of the tasks associated with Certificate lifecycle are delegated to select GlobalSign RAs, who operate on the basis of a service agreement with GlobalSign.

1.3.2. Registration Authorities

GlobalSign performs delegation in accordance with Section 1.3.2 of the GlobalSign CP.

GlobalSign may act as a Registration Authority for Certificates it issues in which case GlobalSign is 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 notarized or otherwise authorized 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 Issuing 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.

RAs may implement more restrictive vetting practices if their internal policy dictates.

GlobalSign may also delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party where permitted by the applicable Industry Standards, except for the following sections, provided that the process as a whole fulfills all of the requirements of Section 3.2:

Certificate type	Source	Section
TLS	Baseline Requirements for TLS	3.2.2.4, 3.2.2.5
EV TLS	EV Guidelines	3.2.2.4, 3.2.2.5
S/MIME BR	Baseline Requirements for S/MIME	3.2.2
Mark	MC Requirements	3.2.14

Before GlobalSign authorizes a Delegated Third Party to perform a delegated function, GlobalSign will contractually require the Delegated Third Party to:

1. Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Abide by the other provisions of the applicable Industry Standards; and
4. Comply with (a) the CA's CP and/or CPS or (b) the Delegated Third Party's practice statement that the CA has verified complies with the Industry Standards and other applicable requirements.

In the case of EPKI (Enterprise PKI) and MSSL (Managed SSL) RAs, Certificates are constrained by a pre-defined and validated GlobalSign 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, the RA must review the validation practices of the third party and Relying Party obligations by referring to such third party's CPS.

1.3.2.1. Enterprise Registration Authorities

GlobalSign may designate an Enterprise RA to verify Certificate requests from the Enterprise RA's own organization, in which case the Subscriber's organization is validated, pre-defined and constrained by system configuration.

GlobalSign may permit the use of Enterprise RA's, subject to the Enterprise RA's agreement with GlobalSign and the requirements in Appendix A of this document.

GlobalSign imposes the limitations applicable to Enterprise Registration Authorities as a contractual requirement on the Enterprise RA and monitors compliance by the Enterprise RA in accordance with Section 8.8.

TLS Certificates

For TLS Certificates, GlobalSign will not accept Certificate requests authorized by an Enterprise RA unless the

following requirements are satisfied:

1. GlobalSign confirms that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.
2. If the Certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, GlobalSign confirms that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject.

Extended Validation Certificates

For Extended Validation TLS or Extended Validation Code Signing Certificates:

1. The Subscriber must be an organization verified by the CA in accordance with the EV Guidelines.
2. GlobalSign shall not delegate the performance of the final cross-correlation and due diligence requirements of Section 3.2.2.13 of the EV Guidelines.

S/MIME BR Certificates

For S/MIME BR Certificates, GlobalSign will not accept Certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. If the Certificate request is for a Mailbox-validated, Organization-validated, or Sponsor-validated profile, GlobalSign confirms that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1 or Section 3.2.2.3.
2. GlobalSign confirms that the subject:organizationName name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject.

An Enterprise RA may also submit Certificate requests using the Mailbox-validated profile for users whose email domain(s) are not under the delegated organization's authorization or control. In this case, GlobalSign confirms that the mailbox holder has control of the requested Mailbox Address(es) in accordance with Section 3.2.2.2.

Mark Certificates

For Mark Certificates, GlobalSign will not accept Certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. GlobalSign confirms that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.
2. If the Certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, GlobalSign confirms that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject.

1.3.3. Subscribers

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.

A *Subscriber*, as used herein, refers to both the Subject of the Certificate and the entity that contracted with GlobalSign for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

Legal Entities are identified on the basis of a review of the entity's published by-laws and appointment of director(s) as well as the subsequent government gazette or similar official government publication or other Qualified Independent Information Source (QIIS) or Qualified Government Information Source (QGIS) third party databases. Self-employed Subjects are identified based on proof of professional registration supplied by the competent authority in the Country in which they reside.

For all categories of Subscribers, additional credentials are required as explained in the online process for the application for a Certificate.

Subscribers of end entity Certificates issued by GlobalSign include employees and agents involved in day-to-day activities within GlobalSign that require access to GlobalSign network resources. Subscribers are also sometimes operational or legal owners of signature creation devices that are issued for the purpose of generating a Key Pair and storing a Certificate.

A Subscriber organization is expected to have a service agreement or other pre-existing contractual relationship with GlobalSign authorizing it to carry out a specific function within the scope of an application that uses GlobalSign Certificate services. Issuance of a Certificate to a Subscriber organization is only permitted pursuant to such an agreement between GlobalSign and the subscribing end entity.

1.3.4. Relying Parties

To verify the validity of a Certificate, Relying Parties must always refer to GlobalSign'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.

Certificates issued by GlobalSign can be used for public domain transactions that require:

- **Non-repudiation/contentCommitment** A party cannot deny having engaged in the transaction or having sent

the electronic message.

- **Authentication** The assurance to one entity that another entity is who he/she/it claims to be.
- **Confidentiality (Privacy)** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- **Integrity** The assurance to an entity that data has not been altered (intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt.

Digital Signature: Digital (Electronic) Signature can only be used for specific transactions that support digital signing of electronic forms, electronic documents, or electronic mail. A Certificate is used to verify the Digital Signature made by the Private Key that matches the Public Key within the Certificate and therefore only in the context of applications that support Certificates. Certificate types that are appropriate for Digital Signatures are the following:

- **PersonalSign 2** Non-repudiation/contentCommitment of a transaction (medium level assurance)
- **PersonalSign 2 Pro** Non-repudiation/contentCommitment of the transaction by a party acting in an organizational context (medium level assurance)
- **AATL** Non-repudiation/contentCommitment of the transaction by a party acting in an organizational context (medium hardware level assurance). (It is not recommended that the Certificate be used for encryption due to the singularity of the Certificate)

Authentication (Users): User authentication Certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail, etc. The authentication function of a Certificate is often the result of a combination of tests on specific properties of the Certificate such as the identity of the Subscriber bound to the Public Key. To describe the function of authentication, the term Digital Signature is often used as this is the method by which the Subscriber can provide a proof of ownership of the Private Key that matches the Public Key within the Certificate.

- **PersonalSign 2** Authentication of a natural person (medium level assurance) and the existence of an email address
- **PersonalSign 2 Pro** Authentication of a natural person within an organizational context or a machine, device, department, or role within an organizational context (medium level assurance) and optionally the existence of an email address
- **PersonalSign 3 Pro** Authentication of a natural person within an organizational context (high level assurance)
- **NAESB Rudimentary** Authentication as prescribed in NIST SP800-63A Digital Identity Guidelines: Enrollment and Identity Proofing, Section 4.3 "Identity Proofing Assurance Level I".
- **NAESB Basic** Authentication as prescribed in the Baseline Requirements for TLS. Section 3.2.3 Authentication of Individual Identity: Employers who verified the identity of their Applicants by means comparable to those stated above for Basic Level may elect to become an LRA and perform identity proofing of Applicants either in-person by inspection of its corporate issued photo ID or through the LRA’s secure online process. The corporate issued photo ID or online process should originate with a government issued photo ID.
- **NAESB Medium** Authentication as prescribed in EV Guidelines. Chapter 3.2.2.2.2(4): Acceptable Method of Verification (4) Principal Individual

Authentication (Devices and Objects): Device authentication Certificates can be used for specific electronic

authentication transactions that support the identification of web sites and other online resources, such as software objects. The authentication function of a Certificate is often the result of a combination of tests on specific properties of the Certificate such as the identity of the device (web server) bound to the Public Key. To describe the function of authentication, the term Digital Signature is often used as this is the method by which, for example, a web server can provide a proof of ownership of the Private Key that matches the Public Key within the Certificate for the Domain Name within the Certificate.

- **DomainSSL** Authentication of a remote Domain Name and webservice and encryption of the communication channel
- **AlphaSSL** Authentication of a remote Domain Name and webservice and encryption of the communication channel
- **OrganizationSSL** Authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel
- **Extended Validation SSL** Authentication of a remote domain name and associated organizational context and webservice and encryption of the communication channel
- **Code Signing** Authentication of a data object with a legal person or a Legal Entity
- **EV Code Signing** Authentication of a data object with a legal person or a Legal Entity
- **Timestamping** Authentication of a time and date related to a service within an organizational context
- **PersonalSign (All)** Authentication of device or machine associated with an organization
- **NAESB Rudimentary** Authentication as prescribed in NIST SP800-63 A Digital Identity Guidelines: Enrollment and Identity Proofing, Section 4.3 “Identity Proofing Assurance Level I.
- **NAESB Basic** Authentication as prescribed in the Baseline Requirements for TLS. Section 3.2.3 Authentication of Individual Identity.
- **NAESB Medium** Authentication as prescribed in the EV Guidelines. Chapter 3.2.2.2.2(4): Acceptable Method of Verification (4) Principal Individual

Assurance Levels: Subscribers should choose an appropriate level of assurance in their identity that they wish to present to Relying Parties. For example, Subscribers with an unknown brand name should positively assure Relying Parties of their identity with an EV Certificate, whereas a closed community with a well-known URL or specific server to server transactions may choose a low assurance level.

- **Low assurance** (Class 1) Certificates are not suitable for identity verification as no authenticated identity information is included within the Certificate. These Certificates do not support non-repudiation/contentCommitment.
- **Medium assurance** (Class 2) Certificates are individual and organizational Certificates that are suitable for securing moderately risky inter and, intra-organizational, and commercial transactions.
- **High assurance** (Class 3) Certificates are individual and organizational Certificates that provide a high level of assurance of the identity of the Subject as compared to Class 1 and 2.
- **High assurance (EV)** Extended Validation Certificates are Class 3 Certificates issued by GlobalSign in conformance with the EV Guidelines.
- **NAESB Rudimentary** This level provides the lowest degree of assurance. One of the primary functions of this level is to provide data integrity of the information being signed. This level is appropriate for environments in

which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where Certificates having higher levels of assurance are unavailable.

- **NAESB Basic** This level provides a basic level of assurance appropriate for environments where there are risks and consequences of data Compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this assurance level that users are not likely to be malicious.
- **NAESB Medium** This level is appropriate for environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.

Confidentiality: All Certificate types, with the exception of timestamping and code signing Certificates, can be used to ensure the confidentiality of communications effected by means of Certificates. Confidentiality may apply to business and personal communications as well as personal data protection and privacy.

Certificates issued under the NAESB PKI may be used for transactions under the WEQ-001, WEQ-002, WEQ-003, WEQ-004, and WEQ-005 business practice standards. They may be used for other transactions by mutual agreement of the parties. Certificates issued under the NAESB Wholesale Electric Quadrant Business Practice Standards WEQ-012 (“NAESB WEQ PKI Standards”) should never be used for performing either of the following functions:

- Any transaction or data transfer that may result in imprisonment if Compromised or falsified; and
- Any transaction or data transfer deemed illegal under federal law

Any other use of a Certificate is not supported by this document: When using a Certificate, the functions of Electronic Signature (non-repudiation/contentCommitment) and authentication (Digital Signature) are permitted together within the same Certificate. The different terms relate to different terminologies used by IETF and the vocabulary adopted within the legal framework of the European Union Directive 1999/93/EC (a Community framework on Electronic Signatures), eIDAS Regulation (Regulation (EU)N910/2014) (“eIDAS”).

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 authorized. Certificates are not authorized for use for any transactions above the designated reliance limits that have been indicated in the GlobalSign Warranty Policy.

Certificates issued under this document do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment on which the Certificate has been installed is not free from defect, malware, or virus. In the case of code signing, Certificates do not guarantee that signed code is free from bugs or vulnerabilities.

Certificates issued under this document shall 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
- Certificates issued under the NAESB WEQ PKI shall never be used for performing either 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 document 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, trademark infringement, 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 CPS Suitability for the Policy

PACOM1 – CA Governance determines the suitability and applicability of the CP and the conformance of this document based on the results and recommendations received from a Qualified Auditor.

In order to maintain credibility and promote trust in this document and better correspond to accreditation and legal requirements, PACOM1 – CA Governance shall review this document 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 document.

1.5.4. CPS Approval Procedures

PACOM1 – CA Governance reviews and approves any changes to the CPS. The updated CPS is reviewed against the CP in order to check for consistency. CP changes are also added on an as-needed basis. Upon approval of a CPS update by PACOM1 – CA Governance, the new CPS 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 CPS.

1.6. Definitions and Acronyms

1.6.1. Definitions

Any terms used but not defined herein shall have the meaning ascribed to them in the Industry Standards and applicable regulation.

Adobe Approved Trust List: 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: means the current versions of the CA/Browser Forum Requirements in Section Introduction.

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

Certificate Authority Authorization: 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.

Certificate 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: A Certificate repository run by Mozilla, where all Publicly-Trusted root and issuing Certificates are listed.

Common Mark Certificate: A Mark Certificate that contains a Mark Representation that has not

been verified as a Registered Mark or Government Mark.

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.

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: 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: A GlobalSign product for organizations to manage the full lifecycle of Microsoft Windows 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

GlobalSign Certificate Center: A cloud-based Certificate management system through which customers and partners may purchase and manage Certificates from GlobalSign.

Global Positioning System: 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.).

Government Mark: A Mark or equivalent granted to or claimed by a government organization (or granted to a Private Organization or other organization) through official statute, regulation, treaty, or government action as it appears or is described in the statute, regulation, treaty, or government action and confirmed by a Mark Verifying Authority using the procedures prescribed in Section 3.2.17.2 of the MC Requirements. A Mark that has been registered by a Government Entity as a trademark with a Trademark Office is not considered a “Government Mark”.

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

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

Hardware Security Module: 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.

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: The applicable requirements defined in Section Industry Standards and Regulations.

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: 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 Common Mark Certificate or Verified Mark Certificate that contains Subject Information and extensions specified in the MC Requirements and that has been verified and issued in accordance with the MC Requirements.

MC Requirements: the current version of the Minimum Security Requirements for Issuance of Mark Certificates published at https://bimigroup.org.

North American Energy Standards Board Accreditation Requirements for Authorized Certification Authorities: 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: 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: A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

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

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

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

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:

- 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: 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: 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 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 Trust Service Provider: 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: A qualified SSL Certificate that meets the requirements of Article 45 of the eIDAS Regulation.

Registered Mark: A type of mark included in a Mark Certificate that meets the requirements of Section 3.2.17.1 of the MC Requirements.

Registration Authority: 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.

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

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

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

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

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.

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.

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 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.

Third Party Validator: An individual or a Legal Entity that is competent and authorized to perform any of the following actions in accordance with national law: 1. to render an opinion on factual claims about the Applicant, including the verification of any specific attributes of the natural or legal person, 2. to authenticate the execution of a signature on a document. Examples may include public officials, notaries, chartered professional accountants, or lawyers.

Trusted Platform Module: 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 Acceptable 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 this document.

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

Verified Mark Certificate: A Certificate that contains Subject Information and extensions specified

in the MC Requirements and that has been verified and issued in accordance with the MC Requirements. Additionally, the Certificate contains a Mark Representation that has been

verified as a Registered Mark or Government Mark.

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

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.

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

1.6.2. Acronyms

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

GCC GlobalSign Certificate Center

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

TPM Trusted Platform Module

VAT Value Added Tax

WEQ Wholesale Electric Quadrant

2. Publication and Repository Responsibilities

2.1. Repositories

GlobalSign publishes this document, Subscriber Agreements, and Relying Party agreements at https://www.globalsign.com/repository which is available on a 24x7 basis. In case of unavailability, GlobalSign aims to make the repository available again within 24 hours.

CRLs are published in online repositories.

Revocation information for Subordinate Certificates and Subscriber Certificates is provided as per Section 4.9.

2.2. Publication of Certification Information

GlobalSign publishes this document, Subscriber Agreements, and Relying Party agreements at https://www.globalsign.com/repository which is available on a 24x7 basis. In case of unavailability, GlobalSign aims to make the repository available again within 24 hours. CRLs are published in online repositories.

Alternative language versions of documents may be available to aid Relying Parties, Subscribers or any other interested party in their understanding; however, in the event of any inconsistency, the English language version shall prevail.

GlobalSign hosts test Web pages that allow Application Software Suppliers and interested parties to test their software with Subscriber Certificates that chain up to each Publicly-Trusted Root Certificate.

Root R1:

https://valid.r1.roots.globalsign.com
https://revoked.r1.roots.globalsign.com
https://expired.r1.roots.globalsign.com

Root R3:

https://valid.r3.roots.globalsign.com
https://revoked.r3.roots.globalsign.com
https://expired.r3.roots.globalsign.com

Root R5:

https://valid.r5.roots.globalsign.com
https://revoked.r5.roots.globalsign.com
https://expired.r5.roots.globalsign.com

Root R6

https://valid.r6.roots.globalsign.com
https://revoked.r6.roots.globalsign.com

https://expired.r6.roots.globalsign.com

Root R46

https://valid.r46.roots.globalsign.com
https://revoked.r46.roots.globalsign.com
https://expired.r46.roots.globalsign.com

Root E46

https://valid.e46.roots.globalsign.com
https://revoked.e46.roots.globalsign.com
https://expired.e46.roots.globalsign.com

2.3. Time or Frequency of Publication

GlobalSign reviews this document at least every 365 days and makes appropriate changes as required.

New or updated versions of repository documents are made publicly available as soon as possible. This typically means within seven days of approval.

2.4. Access Controls on Repositories

GlobalSign makes its Repository publicly available in a read-only manner.

3. Identification and Authentication

GlobalSign verifies and authenticates the identity and other attributes of an Applicant for inclusion in a Certificate.

Applicants are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others. GlobalSign does not verify whether an Applicant has intellectual property rights in the name appearing in the Certificate application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any Domain Name, trademark, trade name or service mark. GlobalSign reserves the right, without liability to any Applicant, to reject an application because of such a dispute.

GlobalSign authenticates requests for Certificate revocation.

3.1. Naming

3.1.1. Types of Names

Certificates are issued with subject DNs (Distinguished Names) in compliance with RFC 5280 and the applicable Industry Standards. DNs respect name space uniqueness.

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. GlobalSign allows common variations or abbreviations of Personal Names consistent with local practice.

3.1.2. Need for Names to be Meaningful

In cases where a GlobalSign product allows the use of a role or departmental name, and where the OU field is included in the DN, additional unique elements may be added to the DN within the OU field to allow Relying Parties to differentiate between Certificates with common DN elements.

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

GlobalSign may issue end entity anonymous or Pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and, where possible, name space uniqueness is preserved. Requests for Internationalized Domain Names (IDNs) in Certificates will be flagged for additional manual review. The decoded hostname will undergo additional review to attempt to mitigate the risk for phishing and other fraudulent usage and the decoded hostname may be compared with previously rejected Certificate requests or revoked Certificates. GlobalSign may reject applications based on risk-mitigation criteria, for instance; names at risk for phishing or other fraudulent usage, names listed on the Google Safe Browsing lists or names listed in the database maintained by the Anti-Phishing Working Group.

GlobalSign allows the use of Pseudonyms for Sponsor-validated S/MIME Certificates in accordance with Section 3.1.3 of the Baseline Requirements for S/MIME i.e. the Pseudonym shall be either a unique identifier selected by the Issuer CA for the Subject of the Certificate, or an identifier selected by the Enterprise RA which identifies the Subject of the Certificate within the Organization included in the subject:organizationName attribute.

GlobalSign reserves the right to disclose a Subscriber's identity when required by law.

3.1.4. Rules for Interpreting Various Name Forms

GlobalSign allows the conversion of Subject Identity Information usually rendered in non-ASCII characters (including Accent or Umlaut-accented characters) using a system commonly used in the Applicant's Jurisdiction of Incorporation or Registration, or recognized by the United Nations or the International Organization for Standardization (ISO). For example, regardless of capitalization:

- Accent characters MAY be represented by their ASCII equivalent. For example é, à, í, ñ, or ç MAY be represented by e, a, i, n, or c, respectively.
- Umlaut-accented characters such as ä, ö, ü MAY be represented by either ae, oe, ue or a, o, u, respectively.

For personal names, GlobalSign MAY include an ASCII character name that is not a direct Conversion of the Applicant's registered name provided that it is verified in a Reliable Data Source or suitable Attestation.

GlobalSign MAY use geographic endonyms and exonyms in the subject:localityName and subject:stateOrProvinceName attributes, (e.g., Munich, Monaco di Bavaria).

3.1.5. Uniqueness of Names

GlobalSign includes a sufficient set of Subject attributes in the Certificate to ensure Subject uniqueness.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of a third party. GlobalSign does not require that an Applicant's right to use a trademark be verified. GlobalSign reserves the right to revoke any Certificate that is involved in a dispute.

3.2. Initial Identity Validation

GlobalSign 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.

GlobalSign uses the results of successful initial identity validation processes to create alternative product offerings by combining elements of previously verified information with alternative, newly verified information. A customer account is used to authenticate the use of any previously verified information for returning Applicants provided that the re-verification requirements of Section 3.3.1 are complied with by the customer account holder.

3.2.1. Method to Prove Possession of Private Key

No stipulation.

3.2.2. Authentication of Organization Identity

GlobalSign maintains internal policies and procedures which are reviewed regularly in order to comply with the requirements of the various root programs that GlobalSign is a member of, as well as the Industry Standards.

Validation policy and procedure documents are under the control of PACOM5 – Subscriber Validation (subordinate to the main Policy Authority in Section 1.5.1) fulfilling the criteria of Principle 6 of the WebTrust Program for CAs. The method by which GlobalSign verifies the organization identity is generally consistent across all product types, however alternative methods, in line with accepted alternatives, may be used where authentication is not possible through the more commonly used QGIS method outlined below.

For all Certificates that include an organization identity, Applicants are required to provide the organization's name and registered or trading address. For all Certificates that include an organization identity, GlobalSign verifies legal existence and identity, legal name, Doing Business As name or tradename or assumed name (if applicable), legal form (where included in the request or part of the legal name in the jurisdiction of incorporation), requested address of the organization and a reliable method of communication. For Extended Validation, GlobalSign additionally verifies physical existence, operational existence and, where required to perform additional validation steps, a reliable means of communication.

This information may be verified using one of the following validation methods:

- A government agency (QTIS or QGIS, including Incorporating Agency or Registration Agency) in the jurisdiction of the Applicant, or a superior governing governmental agency if the Applicant claims they are a government agency themselves.
- A QIIS
- A Verified Legal Opinion or a Verified Accountant Letter
- Independent Confirmation from the Applicant.

Additionally, for non-Extended Validation Certificates, GlobalSign may verify the Applicant's information using one of the following reliable data sources:

- A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information;
- A document, generally a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that has been determined by GlobalSign to be reasonably accurate and reliable. These documents are recognized among commercial enterprises and governments as reliable and are created by a third party for a purpose other than the Applicant obtaining a Certificate; or
- A third party database, created by a third party for a purpose other than the Applicant obtaining a Certificate, that is generally recognized among commercial enterprises and governments as reliable, and that is used to verify information, and which is periodically updated. The third party database is evaluated by GlobalSign for its reliability, accuracy, and resistance to alteration or falsification.

These validation methods are used in accordance with the Industry Standards. Not all validation methods will be acceptable in all circumstances or be available to use for all types of information.

The list of Incorporating Agencies or Registration Agencies is published in the Legal Repository on GlobalSign's website (globalsign.com), under the section "Validation Resources".

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

3.2.2.1. Local Registration Authority Authentication

For EPKI and MSSL accounts, GlobalSign sets authenticated organizational details in the form of a *Profile.* Suitably authenticated account administrators acting in the capacity of a Local Registration Authority authenticate individuals Affiliated with the organization and/or any sub-domains owned or controlled by the organization. *(While LRAs are able to authenticate individuals under contract, all domains to be authenticated will have previously been verified by GlobalSign).*

3.2.2.2. Role Based Certificate Authentication (DepartmentSign)

GlobalSign ensures that requests for machine, device, department, or role-based Certificates are authenticated. LRAs are contractually obligated to ensure that machine, device, department, or role-based names relating to the organization profile and its business are accurate and correct.

3.2.2.3. S/MIME BR Certificates

The Applicant's information includes the following:

- Formal name of the Legal Entity;
- A registered Assumed Name for the Legal Entity (optional)
- An Affiliate of the Legal Entity (optional);
- An address of the Legal Entity;
- Organization Identifier, consisting of an appropriate Registration Scheme identifier, 2 character ISO 3166 country code for the nation where the scheme is operated ("XG" shall be used when the scheme is operated globally), where applicable the ISO 3166-2 identifier for the subdivision of the nation in which the Registration Scheme is operated, and where applicable the registration reference allocated in accordance with the identified Registration Scheme.

GlobalSign verifies the Applicant's information using at least one of the following methods:

1. A government agency in the jurisdiction of the Legal Entity's creation, existence, or recognition;
2. A Legal Entity Identifier (LEI) data reference;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation which includes a copy of supporting documentation used to establish the Applicant's legal existence (such as a Certificate of registration, articles of incorporation, operating agreement, statute, or

regulatory act) and its current status.

In cases 1 and 4 above, GlobalSign verifies that the status of the Applicant is not designated by labels such as "ceased," "inactive," "invalid," "not current," or the equivalent.

In case 2 above when LEI data reference is used, GlobalSign verifies that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. GlobalSign only allows use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI will not be used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

GlobalSign uses the following Registration Schemes:

- NTR: For an identifier allocated by a national or state trade register to the Legal Entity named in the subject:organizationName.
- VAT: For an identifier allocated by the national tax authorities to the Legal Entity named in the subject:organizationName.
- LEI: For a Legal Entity Identifier as specified in ISO 17442 for the entity named in the subject:organizationName. The 2 character ISO 3166 country code shall be set to ‘XG'
- GOV: For Government Entities
- INT: for Non Commercial Entities. The 2 character ISO 3166 country code shall be set to ‘XG'

GlobalSign verifies Assumed Names by verifying that:

- The Applicant has registered its use of the Assumed Name with the appropriate government agency for such filings in the jurisdiction of its incorporation or registration; and
- The Assumed Name filing continues to be valid.

GlobalSign may rely on an attestation that indicates the Assumed Name under which the Applicant conducts business, the government agency with which the Assumed Name is registered, and that such filing continues to be valid.

3.2.2.4. Mark Certificates

GlobalSign validates the following in accordance with the Minimum Security Requirements for Issuance of Mark Certificates (relevant sections referenced below):

- The Applicant’s existence and identity, including;
  - Applicant’s legal existence and identity (See Section 3.2.5. Verification of Applicant’s Legal Existence and Identity)
  - If applicable, Applicant’s Assumed name (See Section 3.2.6. Verification of Applicant’s Legal Existence and Identity - Assumed Name)
  - Applicant’s physical existence (business presence at a physical address) See section (3.2.7. Verification of Applicant’s Physical Existence),
  - Applicant’s operational existence (business activity) (See Section 3.2.9. Verification of Applicant’s

Operational Existence).

- That Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the Mark Certificate (See Section 3.2.14. Validation of Domain Authorization or Control);
- A reliable means of communication with the entity to be named as the Subject in the Certificate (See Section 3.2.8. Verified Method of Communication);
- The Applicant's authorization for the Mark Certificate, including:
  - name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester (See Section 3.2.10. Verification of Identity and Authority of Contract Signer and Certificate Approver),
  - Contract Signer signed the Subscriber Agreement or that a duly authorized individual acknowledged and agreed to the Terms of Use (See Section 3.2.11. Verification of Signature on Subscriber Agreement and Mark Certificate Requests);
  - Certificate Approver has signed or otherwise approved the Certificate Request. (See Section 3.2.12. Verification of Approval of Mark Certificate Request)
  - F2F Verification Procedure (See sections G.1 and G.2)
- The Applicant's Mark (See sections 3.2.16. Mark Verification in Common Mark Certificates and 3.2.17. Mark Verification in Verified Mark Certificates)

GlobalSign uses the following information sources:

- Verified Legal Opinion (See Section 3.2.13.1. Verified Legal Opinion)
- Verified Accountant Letter (See Section 3.2.13.2. Verified Accountant Letter)
- Face-to-Face Validation (See Section 3.2.13.3. Face-to-Face Validation using the Notarization process)
- Independent Confirmation From Applicant (See Section 3.2.13.4. Independent Confirmation From Applicant)
- Qualified Independent Information Source (See Section 3.2.13.5. Qualified Independent Information Source)
- Qualified Government Information Source (See Section 3.2.13.6. Qualified Government Information Source)
- Qualified Government Tax Information Source (See Section 3.2.13.7. Qualified Government Tax Information Source)

Additionally, GlobalSign performs the following checks:

- Denied Lists and Other Legal Block Lists (See Section 3.2.18.1. Denied Lists and Other Legal Block Lists)
- Parent/Subsidiary/Affiliate Relationship (See Section 3.2.18.2. Parent/Subsidiary/Affiliate Relationship)

For every Certificate Request, the Subject information is subject to Cross-Correlation and Due Diligence checks in accordance with Section 3.2.19. Final Cross-Correlation and Due Diligence.

3.2.2.5. Qualified Certificates

GlobalSign issues the following Qualified Certificates that include an Organization Identity:

- 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 administrator acting in the capacity of a Local Registration Authority.

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

GlobalSign will verify the authority of the authorized 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 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 authorized representative in accordance with Section 3.2.3.

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

GlobalSign may issue Certificates from its production environment intended for testing and/or auditing, following the same processes and procedures as regular Certificates. These Certificates shall be revoked after testing to ensure they cannot be used outside of the testing scope.

For any PSD2 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 Certificate file.

3.2.3. Authentication of Individual identity

GlobalSign authenticates Individuals depending upon the class of Certificate as indicated below.

3.2.3.1. Class 1

The Applicant is required to demonstrate control of their email address or domain name to which the Certificate relates. GlobalSign does not authenticate additional information/attributes which may be provided by the Applicant during the application and enrollment process. This encompasses DV Certificates.

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

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. This encompasses OV Certificates.

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

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:

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

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

- 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;
- 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 confirms 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;
- 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;
- 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; or
- Other verifications in line with the verification of individuals for Qualified Certificates.

For AATL, GlobalSign may establish the Individual's identity and perform inspection of a Governmentally Accepted Form of ID through a video-based meeting or an approach with equivalent assurance.

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 in 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 (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 or a Trusted Third Party 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.

Where the submission of a copy of a government issued national identity document or photo ID is prohibited by local law or regulation, GlobalSign shall use an alternative method to authenticate the identity of the Applicant. In such cases, GlobalSign shall accept attestation or documentation from a Trusted Third Party authorized to conduct identity verification.

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.

GlobalSign may establish the Individual's identity and perform inspection of a Governmentally Accepted Form of ID through a video-based meeting or an approach with equivalent assurance.

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

GlobalSign also authenticates 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 demonstrate an equivalent level of confidence.

3.2.3.4. S/MIME BR Certificates

Applicant's information includes the following:

1. Given name(s) and surname(s), which shall be current names;
2. Pseudonym (if used);
3. Title (if used); and
4. Further information as needed to uniquely identify the Applicant.

GlobalSign must verify the Individual Applicant's identity and identity attributes information using at least one of the following methods:

- For the collection of Applicant's identity and identity attributes:
  - Using an official physical identity document, issued to the Applicant by a relevant government agency in the Applicant's jurisdiction, for the purposes of identification, containing a photo and/or other (biometric) information that can be compared with the Applicant's physical appearance. Examples include but are not limited to passports, identity cards, drivers' licenses and military IDs. (S/MIME BR Section 3.2.4.1 (1)); or
  - Using a digital or electronic identity document, considered eMRTD identity documents according to ICAO 9303 part 10 (S/MIME BR Section 3.2.4.1 (2)); or
  - Using a valid eID issued under a "notified" eID schemes according to Article 9 of the eIDAS Regulation and the eID shall conform to eIDAS LoA "Substantial" or "High" (S/MIME BR Section 3.2.4.1 (3)); or
  - Using a Certificate request signed with a valid Digital Signature, based on a valid personal Certificate that was issued under an Approved Framework described in the S/MIME BRs (S/MIME BR Section 3.2.4.1 (4)); or
  - For Sponsor-validated Certificates only, using Enterprise RA records (S/MIME BR Section 3.2.4.1 (5)).
  - For authority or affiliation of an Individual to represent an Organization to be included in the subject:organizationName of the Certificate, using an Attestation provided by the Organization (S/MIME BR Section 3.2.4.1 (6)).
  - Using an Attestation from a qualified legal practitioner or notary in the Applicant's jurisdiction (S/MIME BR Section 3.2.4.1 (7)).

GlobalSign shall verify supplementary evidence using authorized sources such as additional official documents, government or regulatory registers, or national population registers (S/MIME BR Section 3.2.4.1 (8)). Before relying on a source of verification data, GlobalSign verifies its suitability as a Reliable Data Source.

In terms of validation, the following practices apply:

Any physical identity document shall be presented in its original form. GlobalSign employs procedures to ensure the evidence presented by the Applicant is a genuine identity document that is not counterfeited or falsified/modified. When using a remote process, this process ensures that the Applicant has the document in hand and presents the document in real-time in front of a camera. GlobalSign maintains an internal authoritative source of information which covers documents accepted by GlobalSign, their appearance and how to validate these documents. (S/MIME BR Section 3.2.4.2 (1))

For digital identity documents, GlobalSign checks that the issuer's Digital Signature on the document is successfully validated according to ICAO 9303 part 11. (S/MIME BR Section 3.2.4.2 (2))

For both physical and digital identity documents, GlobalSign may use manual (in person) or remote procedures, or a combination of both. GlobalSign records the following information: issuer, validity period, and the document's unique identification number. To ensure that the Applicant's identity is verified, GlobalSign makes a visual comparison of the physical appearance of the Applicant and the face photo and/or other information on the physical or digital identity document. (S/MIME BR Section 3.2.4.2 (1) and 3.2.4.2 (2))

For authentication using the eID, the validation with the eID's Identity Provider (IdP) is documented and retained (S/MIME BR Section 3.2.4.2 (3)).

For validation of a Digital Signature with a Certificate, the signature shall have been created as part of the identity

validation process. GlobalSign validates the Digital Signature and only uses the signing Certificate as evidence for identity attributes if the signature is valid (S/MIME BR Section 3.2.4.2 (4)).

For validation of an attestation, GlobalSign verifies the reliability of the Attestation Letter in accordance with Section 3.2.8 of the Baseline Requirements for S/MIME. GlobalSign verifies that the Attestation was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information. An Attestation includes a copy of documentation supporting the fact to be attested. GlobalSign uses a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic (S/MIME BR Section 3.2.4.2 (5)).

For validation using an Enterprise RA Record, the Enterprise RA issuing a Sponsor-validated Certificate validates all identity attributes of an Individual to be included in the Certificate. The Enterprise RA may rely upon existing internal records to validate Individual identity (S/MIME BR Section 3.2.4.2 (6)).

3.2.3.5. Qualified Certificates

GlobalSign verifies the Identity of Individual Subscribers according to Article 24.1 of the eIDAS Regulation, in particular using the following methods:

- In-person identity verification
- Using electronic identification means
- Using Qualified Electronic Signature

In-person Verification

In-person verification requires a physical presence of the Subscriber, and requires the production of the following documents:

- Government Issued Photo ID
- Signed personal statement

The likeness of the Individual is compared to the Photo ID, and the security features of the Photo ID are inspected. The signature on the personal statement is compared to the signature on the Photo ID.

This verification may be performed by a Third Party Validator.

Additional secondary evidence may be required to ensure the uniqueness of the Applicant's identity, or to validate information included in the Certificate other than the given name.

Using Remote Electronic Identification Means

GlobalSign may use electronic identification means to verify the Individual Identity. All electronic identification means have an assurance level of 'Substantial' or 'High' as set out in Article 8 of the eIDAS Regulation. Prior to issuance, the physical presence of the Individual is ensured.

1. For notified electronic identification schemes, the assurance level will be determined by the notification given by the Member State to the Commission.

2. For electronic identification means that have not been notified, the assurance level will be determined according to the factors described by the European Commission. After review by the Conformity Assessment Body, GlobalSign will present the findings to the Supervisory Body for acceptance prior to accepting the electronic identification means in this section.

Qualified Electronic Signature

GlobalSign uses the Subscriber's valid qualified Electronic Signature on a personal statement to verify the Applicant's identity and additional attributes contained in the Certificate used to create the qualified Electronic Signature. The Certificate must be issued in compliance with Article 24 (a) or (b) of the eIDAS Regulation.

3.2.3.6. Local Registration Authority Authentication

For Organization accounts which allow the concept of a Local Registration Authority, GlobalSign sets 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 using Certificates for WEQ-012 applications 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. 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 document 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

GlobalSign does not verify the contents of the Subject:OrganizationalUnitName field, except for Code Signing Certificates where the Subject:OrganizationalUnitName field contains a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity.

GlobalSign may allow the use of the Subject:SerialNumber as a location for non-verified Subscriber information where permitted by Industry Standards.

For IntranetSSL SSL Certificates only, GlobalSign relies 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.

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

3.2.5. Validation of Authority

Certificate type	Method
PersonalSign1 Certificates	Verification that the Applicant has control over the email address to be listed within the Certificate through a challenge response mechanism.
PersonalSignDemo 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.)

Certificate type	Method
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 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.
PersonalSign3 Certificates	Verification through a reliable means of communication with the Applicant Representative that they have 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, 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.
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 through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address that may be optionally listed within the Certificate.
EV Code Signing Certificates	Verifying the authority of the contract signer and Certificate approver in accordance with the EV Guidelines 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.

Certificate type	Method
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 authorized 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.
Mark Certificates	Verifying the authority of the contract signer and Certificate approver in accordance with the methods listed in Section 3.2.2.4.

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

- an advanced (or higher) Electronic Seal which includes the name of the organization, its parent, subsidiary or Affiliate; or
- an advanced (or higher) Electronic Signature which includes the name of the organization, its parent, subsidiary or Affiliate. In this case, GlobalSign will verify that the individual has been appropriately verified as either a confirmed employee or an agent of the organization listed in the Certificate; or
- an advanced (or higher) Electronic Signature of a confirmed employee or agent of the organization.

3.2.6. Criteria for Interoperation

Cross Certificates are published in the GlobalSign Repository.

3.2.7. Authentication of Domain Names

For all instances of verification of control or ownership of the domain except for Mark Certificates, authentication of the Applicant's (or the Applicant's parent company's, subsidiary company's, or Affiliate's, collectively referred to as "Applicants" for the purposes of this section) ownership or control of all requested FQDN(s) is done using one of the following methods of Section 3.2.2.4 of the Baseline Requirements for TLS:

- Constructed Email to Domain Contact (3.2.2.4.4); or
- DNS Change (3.2.2.4.7); or
- Email to DNS CAA Contact (3.2.2.4.13); or
- Email to DNS TXT Contact (3.2.2.4.14); or
- Phone Contact with DNS TXT Record Phone Contact (3.2.2.4.16); or
- Agreed-Upon Change to Website v2 (3.2.2.4.18), or

- Agreed-Upon Change to Website - ACME (3.2.2.4.19)

GlobalSign uses the methods above except for method 9 (TLS BR 3.2.2.4.18) and method 10 (TLS BR 3.2.2.4.19) for validating Wildcard FQDNs. Following redirects is supported for methods 9 (TLS BR 3.2.2.4.18 and 10 (TLS BR 3.2.2.4.19).

For all instances of verification of control or ownership for Mark Certificates, authentication of the Applicant's (or the Applicant's parent company's, subsidiary company's, or Affiliate's, collectively referred to as "Applicants" for the purposes of this section) ownership or control of all requested FQDN(s) is done using one of the following methods of Section 3.2.14 of the MC Requirements:

- Constructed Email to Domain Contact (3.2.14.4); or
- DNS Change (3.2.14.7); or
- Email to DNS CAA Contact (3.2.14.13); or
- Email to DNS TXT Contact (3.2.14.14); or
- Phone Contact with DNS TXT Record Phone Contact (3.2.14.16); or
- Agreed-Upon Change to Website v2 (3.2.14.18), or
- Agreed-Upon Change to Website - ACME (3.2.14.19)

Following redirects is supported for methods MCRs 3.2.14.18 and MCRs 3.2.14.19.

GlobalSign maintains a record of the validation method used to validate every domain address in issued Certificates.

DNSSEC validation is performed for Publicly-Trusted TLS and S/MIME Certificates in accordance with Baseline Requirements for TLS Section 3.2.2.4.

3.2.8. Authentication of IP Addresses

GlobalSign uses the following methods of Section 3.2.2.5 of the Baseline Requirements for TLS to confirm that the Applicant has control of or right to use IP Addresses:

1. Agreed-Upon Change to Website (3.2.2.5.1); or
2. Email, Fax, SMS, or Postal Mail to IP Address Contact (3.2.2.5.2); or,
3. Reverse Address Lookup (3.2.2.5.3); or
4. Phone Contact with IP Address Contact (3.2.2.5.5).

GlobalSign maintains a record of the validation method used to validate every IP Address in issued Certificates.

3.2.9. Authentication of Email Addresses

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

1. Verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate (S/MIME BR Section 3.2.2.1); or
2. Confirming the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value (S/MIME BR Section 3.2.2.2).

GlobalSign maintains a record of the validation method used to validate every email address in issued Certificates.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

For products supporting re-key, authentication of the re-key request is based on the authentication mechanism provided during the initial issuance of the Certificate, or equivalent.

Identification of the request is subject to the re-use conditions specified in Section 4.2.1. If at any point any information included 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

Identification and authentication of revocation requests is performed as per Section 4.9.

Requests initiated by GlobalSign do not require identification and authentication.

4. Certificate Lifecycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

GlobalSign maintains criteria and internal databases, including individuals from whom and entities from which it will not accept Certificate applications. In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which GlobalSign operates are used to screen out unwanted Applicants.

GlobalSign does not issue Certificates to entities that reside in Countries where the laws of a GlobalSign office location prohibit doing business.

The EV Guidelines highlight the specific rules to follow in order to obtain an Extended Validation SSL / Extended Validation Code Signing Certificate. Applicants must submit and agree to a Certificate request and Subscriber Agreement, which may be electronic or pre-authorized depending upon the nature of the service required from GlobalSign.

4.1.2. Enrollment Process and Responsibilities

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

GlobalSign maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow GlobalSign and any GlobalSign RA to successfully perform the required verification. GlobalSign and RAs shall protect communications and securely store information presented by the Applicant during the application process in compliance with the GlobalSign Privacy Policy.

Generally, the application process includes the following steps (but not necessarily in this order as some workflow processes generate Key Pairs after the validation has been completed):

- Generating a suitable Key Pair using a suitably secure platform;
- Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
- Submitting a request for a Certificate type and appropriate application information;
- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
- Paying any applicable fees.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

GlobalSign maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this document.

Initial identity vetting may be performed by GlobalSign's validation team as set forth in Section 3.2 or by Registration Authorities under contract. All communications sent through via fax or email are securely stored along with all information presented directly by the Applicant via the GlobalSign web interface or API. Future applications for Certificates are authenticated using single (username and password) or multi-factor (Certificate in combination with username/password) authentication techniques.

GlobalSign may use the documents and data provided in Section 3.2 to verify Certificate information, or may reuse previous validations themselves, provided that:

- For TLS, S/MIME BR and Code Sign Certificates, GlobalSign obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate. For TLS Certificates issued on or after March 15, 2026, the reuse period is 398 days;
- For S/MIME BR Certificates, for validation of mailbox authorization or control: any reused data, document, or completed validation has been obtained no more than 30 days prior to issuing the Certificate;
- For SSL Certificates, for validation of Domain Names and IP Addresses according to Section 3.2.2.4 and 3.2.2.5 of the Baseline Requirements for TLS, any reused data, document, or completed validation has been obtained no more than 398 days prior to issuing the Certificate. For TLS Certificates issued on or after March 15, 2026, the reuse period is 200 days; and
- For EV SSL and EV Code Signing Certificates, GlobalSign obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 398 days prior to issuing the Certificate. Except for reissuance of an EV Certificate under Section 3.2.2.14.2 and except when permitted otherwise in Section 3.2.2.14.1 of the EV Guidelines.
- For Qualified Certificates:
  - GlobalSign obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 398 days prior to issuing the Certificate; or
  - Regardless of age of validated data, GlobalSign may rely on a previously verified Certificate request to issue a replacement Certificate, so long as the Certificate being referenced was not revoked due to fraud or other illegal conduct, if:
    - The expiration date of the replacement Certificate is the same as the expiration date of the Qualified Certificate that is being replaced, and
    - The Subject Information of the Certificate is the same as the Subject in the Qualified Certificate that is being replaced.
- For Mark Certificates, GlobalSign obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 398 days prior to issuing the Certificate, except for:
  - An authorization letter from the owner of record of the Registered Mark or Government Mark (as described in Section 3.2.17.1.2 and Section 3.2.17.2.2 of the Minimum Security Requirements for Issuance of Mark Certificates) may be reused for up to 1,858 days.

- Regardless of age of validated data, face-to-face validation may be re-used for any Subscriber Organization (or Parent, Subsidiary, or Affiliate) in accordance with Section 4.2.1. of the Minimum Security Requirements for Issuance of Mark Certificates. GlobalSign maintains continuous contact by sending email notification to Subscribers prior to the expiry of their Certificate informing Subscribers about upcoming expiration of their Certificates to an email address chosen by the Subscriber.

In some cases, GlobalSign may rely on a contract with the Applicant that specifies a different term for the validation of authority, verified in accordance with Section 3.2.5. For example, the contract may include the perpetual assignment of roles until revoked by the Applicant or CA, or until the contract expires or is terminated. GlobalSign may establish a process that allows an Applicant to specify the Individuals who may request Certificates. In case of Local Registration Authorities, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile. This authority may remain valid until revoked.

Customers may request a replacement Certificate (“reissue”), which follows the process of a new Certificate. Where applicable, Certificate information may be reused.

If at any point any Subject name information embodied in a Certificate is changed in any way, the procedures outlined herein must be re-performed.

GlobalSign develops, maintains, and implement documented procedures to flag Certificate requests for additional scrutiny prior to the Certificate’s approval, by reference to its internal criteria and databases, which may include:

- names at higher risk for phishing or other fraudulent usage;
- names contained in previously rejected Certificate requests or revoked Certificates; or
- the factors that GlobalSign identifies using its own risk-mitigation criteria.

4.2.2. Approval or Rejection of Certificate Applications

GlobalSign shall reject requests for Certificates where validation of all items cannot be successfully completed.

Assuming all validation steps can be completed successfully following the procedures in this document, then GlobalSign shall generally approve the Certificate request. GlobalSign may reject applications including for the following reasons:

- GlobalSign may reject requests based on potential brand damage to GlobalSign in accepting the request.
- GlobalSign may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement.

GlobalSign is under no obligation to provide a reason to an Applicant for rejection of a Certificate request.

For Extended Validation, Qualified and Code Signing Certificates, separation of duties requires two members of the validation team to approve the request. GlobalSign operates in many jurisdictions; however, it may choose to outsource a pre-vetting function to suitably trained and experienced external RA partners who have additional relevant language and local jurisdiction knowledge to be able to process and/or translate documentation that is not in a language that GlobalSign itself can process internally.

GlobalSign does not issue Publicly-Trusted TLS Certificates to Internal Names or Reserved IP Addresses.

GlobalSign does not issue Publicly-Trusted Mark Certificates containing Internal Names.

4.2.2.1. Certification authority authorization

GlobalSign validates each FQDN in a Publicly-Trusted TLS, S/MIME and Mark Certificate against the domain's CAA records. GlobalSign's CAA issuer domain is "globalsign.com".

For TLS Certificates, prior to issuing a Certificate, GlobalSign retrieves and processes CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name.

For S/MIME Certificates, prior to issuing a Certificate that includes a Mailbox Address, GlobalSign retrieves and processes CAA records in accordance with RFC 9495. If the Certificate includes more than one Mailbox Address, then GlobalSign processes the CAA records for each Mailbox Address.

For Mark Certificates, prior to issuing a Certificate, GlobalSign retrieves and processes CAA records in accordance with RFC 8659 for each FQDN to be included in a dNSName within the Mark Certificate's subjectAlternativeName extension.

If CAA record(s) exist, GlobalSign will only issue a Certificate when a CAA record exists that contains "globalsign.com".

GlobalSign:

- caches CAA records for reuse for up to 8 hours
- supports the issue, issuewild, issuemail and issuevmc CAA tags
- processes but does not act on iodef property tag (i.e., GlobalSign does not dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s))
- does not support any additional property tags

GlobalSign documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances.

DNSSEC validation is performed for Publicly-Trusted TLS and S/MIME Certificates in accordance with Baseline Requirements for TLS Section 3.2.2.8.1 and Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates 4.2.2.1.1.

4.2.3. Time to Process Certificate Applications

GlobalSign shall ensure that all reasonable methods are used to evaluate and process Certificate applications. Where issues outside of the control of GlobalSign occur, GlobalSign shall strive to keep the Applicant duly informed.

For Extended Validation Certificates, GlobalSign first validates that all information provided by the Applicant is correct before requesting the contract signer to approve the Subscriber Agreement.

The following approximations are given for processing and issuance.

- **PersonalSign1 Certificates** Approximately 1 minute
- **PersonalSign2 Certificates** Approximately 24-48 business hours
- **PersonalSign2 Pro Certificates** Approximately 36-72 business hours
- **NAESB Certificates** Approximately 24-48 business hours
- **PersonalSign3 Pro Certificates** Approximately 48-72 business hours
- **Code Signing Certificates** Approximately 24-48 business hours
- **EV Code Signing Certificates** Approximately 48-96 business hours
- **DV SSL Certificates** Approximately 1-5 minutes
- **AlphaSSL Certificates** Approximately 1-5 minutes
- **OV SSL Certificates** Approximately 24-48 business hours
- **EV SSL Certificates** Approximately 48-96 business hours
- **Qualified Certificates** Approximately 48-96 business hours
- **Mark Certificates** Approximately 48-96 business hours
- **Timestamping Certificates** Approximately 5-10 business days
- **AATL Certificates** Approximately 24-48 business hours
- **S/MIME Certificates** Approximately 48-72 business hours

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 issue a direct command for the Root CA to perform a Certificate signing operation.

GlobalSign shall ensure it communicates with any RA accounts capable of causing Certificate issuance using multi-factor authentication. This includes RAs directly operated by GlobalSign or RAs contracted by GlobalSign. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorized modification or tampering.

For publicly-trusted TLS and Mark Certificates, GlobalSign logs the Certificate pre-Certificate to one or more public CT logs within 24 hours of issuance.

4.3.1.1. Linting of to-be-signed and issued Certificate content

For Publicly-Trusted TLS, S/MIME and Mark Certificates, GlobalSign performs linting on the Precertificate (where applicable), to-be-signed Certificate and issued Certificate using Linting tools that have been widely adopted by the industry.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

GlobalSign or RA shall notify the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrollment process or by any other equivalent method. The email may contain the Certificate itself or a link to download depending upon the workflow of the Certificate requested.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

GlobalSign 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. Unless the Subscriber notifies GlobalSign within seven (7) days from receipt, the Certificate is deemed accepted.

4.4.2. Publication of the Certificate by the CA

GlobalSign publishes the Certificate by delivering it to the Subscriber and may also publish to one or more Certificate Transparency Logs. In addition, for Enterprise PKI customers GlobalSign may publish the Certificate into a directory such as LDAP.

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, except for Mark Certificates, for which the Private Key does not need to be protected and may be discarded.

GlobalSign's Subscriber Agreement identifies the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate.

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.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties must accept and act in accordance with the requirements in Section 9.6.4 prior to reliance upon a Certificate from GlobalSign. 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.

Certificate renewal requests are processed as new Certificate requests when Subscriber or other participant's Public Key or any other information in the Certificate is different.

4.6.1. Circumstances for Certificate Renewal

If supported for the product, Certificate renewal may be performed upon request of the Subscriber, an authorized representative of Subscriber or by GlobalSign at its sole discretion.

Certificate renewal can 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, GlobalSign verifies the request with Subscriber or their authorized representative.

Certificate renewal requests are processed as new Certificate requests.

4.6.4. Notification of New Certificate Issuance to Subscriber

As per Section 4.3.2

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

As per Section 4.4.1

4.6.6. Publication of the Renewal Certificate by the CA

As per Section 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.

Certificate re-key requests are processed as new Certificate requests when the validity period is changed or any other information in the Certificate is different.

4.7.1. Circumstances for Certificate Re-Key

If supported for the product, Certificate re-key may be performed upon request of the Subscriber, an authorized representative of Subscriber or by GlobalSign 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, GlobalSign verifies the request with the Subscriber or their authorized representative.

Certificate re-key requests are processed as new Certificate requests.

4.7.4. Notification of New Certificate Issuance to Subscriber

As per Section 4.3.2

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

As per Section 4.4.1

4.7.6. Publication of the Re-Keyed Certificate by the CA

As per Section 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.

Certificate modification requests are processed as new Certificate requests when the validity period is changed or the Subscriber Public Key is different.

4.8.1. Circumstances for Certificate Modification

If supported for the product, Certificate modification may be performed upon request of the Subscriber, an authorized representative of Subscriber or by GlobalSign 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, GlobalSign verifies the request with Subscriber or their authorized representative.

Certificate modification requests are processed as new Certificate requests.

4.8.4. Notification of New Certificate Issuance to Subscriber

As per Section 4.3.2

4.8.5. Conduct Constituting Acceptance of Modified Certificate

As per Section 4.4.1

4.8.6. Publication of the Modified Certificate by the CA

As per Section 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, GlobalSign will verify the authenticity of the revocation request.

GlobalSign may revoke any Certificate at its sole discretion.

Revocation of a Subscriber Certificate is performed within twenty-four (24) hours under the following circumstances:

1. The Subscriber requests in writing (to GlobalSign which provided the Certificate) that they wish to revoke the Certificate;
2. The Subscriber notifies GlobalSign that the original Certificate request was not authorized and does not retroactively grant authorization;
3. GlobalSign obtains reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. GlobalSign 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. GlobalSign 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. GlobalSign obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon;
7. GlobalSign receives notice or otherwise becomes aware of unexpected termination of a Subscriber's or Subject's agreement or business functions; or
8. In case of PSD2 Certificates, GlobalSign 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.

Revocation of a Subscriber's Certificate should be performed within twenty-four (24) hours and is performed 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. GlobalSign obtains evidence that the Certificate was misused;
3. GlobalSign receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;

4. GlobalSign 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. GlobalSign 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. GlobalSign receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
7. GlobalSign is made aware that the Certificate was not issued in accordance with the applicable Industry Standards or GlobalSign's CP or CPS;
8. GlobalSign determines that any of the information appearing in the Certificate is inaccurate;
9. GlobalSign's right to issue Certificates under the applicable Industry Standards expires or is revoked or terminated, unless GlobalSign has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by GlobalSign's CP and/or CPS;
11. GlobalSign 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;
12. GlobalSign is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
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. GlobalSign receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the Certificate is no longer legally permitted;
15. The CA Private Key used in issuing the Certificate is suspected to have been compromised;
16. GlobalSign ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
17. The Certificate was issued in violation of the then-current version of the Mozilla Root Store Policy; or
18. 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 Mark Certificate 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 GlobalSign's support team or

GlobalSign's Registration Authority;

3. GlobalSign 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 GlobalSign's jurisdiction of operation;
4. The Subscriber was added as a denied party or is otherwise designated or subject to economic sanctions or other restrictions pursuant to applicable laws;
5. Overdue payment of applicable fees by the Subscriber;
6. Following the request for cancellation of a Certificate;
7. If a Certificate has been re-issued, GlobalSign may revoke the previously issued Certificate;
8. Under certain licensing arrangements, GlobalSign may revoke Certificates following expiration or termination of the license agreement;
9. GlobalSign 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 GlobalSign's or a third party's business or reputation, GlobalSign will consider, among other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force, and responses to the alleged harmful use by the Subscriber;
10. 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; or
11. 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 in writing to the GlobalSign entity which provided the Subordinate CA Certificate, or the authority detailed in Section 1.5.2 of this document, that GlobalSign revoke the Certificate;
2. The Subscriber notifies GlobalSign that the original Certificate request was not authorized and does not retroactively grant authorization;
3. GlobalSign 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. GlobalSign obtains evidence that the Certificate was misused;
5. GlobalSign 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. GlobalSign determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. GlobalSign or a Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
8. GlobalSign's or a 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; or
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).

If Subscriber requests revocation, the applicable revocation reason can be provided:

- Unspecified: When the reason codes below do not apply to the revocation request, the Subscriber must not provide a reason code other than "unspecified";
- keyCompromise: When there is reason to believe that the Private Key of their Certificate has been compromised, e.g. an unauthorized person has had access to the Private Key of their Certificate;
- cessationOfOperation: When they no longer own all of the domain names in the Certificate or when they will no longer be using the Certificate because they are discontinuing their website;
- affiliationChanged: When their organization's name or other organizational information in the Certificate has changed; or
- Superseded: When they request a new Certificate to replace their existing Certificate.

If the revocation reason is not specified by the Subscriber, the "unspecified" revocation reason is used.

For short-term Certificates issued through the GlobalSign Document Signing Service and Qualified Signing Service, revocation by the Subscriber is not supported.

4.9.2. Who Can Request Revocation

GlobalSign, RA or Subscriber can initiate revocation. Only authenticated requests for revocation are accepted. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an Affiliated organization named in the Certificate. Subscribers, Relying Parties, Application Software Suppliers, Conflicting Trademark Owners, and other third parties may submit Certificate Problem Reports to notify GlobalSign of a suspected reasonable cause to revoke the Certificate. Additionally, for Open Banking Certificates, revocation requests can originate from the NCA which has authorized or registered the payment service provider. GlobalSign may also at its own discretion revoke Certificates including Certificates that are issued to other cross signed CAs.

4.9.3. Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, GlobalSign provides automated mechanisms for requesting and authenticating revocation requests. The primary method is through the customer account used to issue the Certificate that is requested to be revoked. Alternative out of band methods may be used, such as receipt of a fax/letter/phone call, the origins of which must be authenticated using shared secrets from the customer account. Alternatively, where customer accounts are not provided, methods may be used which rely on a demonstration of control of one or more elements of the Subject DN of the Certificate. For S/MIME Certificates, it could include demonstration of control of the email address. GlobalSign and its RAs will record each request for

revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved.

Subscribers, Relying Parties, Application Software Suppliers, Conflicting Trademark Owners and other third parties may submit a Certificate Problem Report via report-abuse@globalsign.com. GlobalSign may or may not revoke in response to this request. See Section 4.9.5 for detail of actions performed by GlobalSign for making this decision.

If revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this document.

4.9.3.1. Certificate Problem Reports

Claims made in the Certificate Problem Report must be supported with sufficient information to allow GlobalSign to identify the reported Certificate or specific Subscriber, and to verify the details of the claims.

For the identity of the reported Certificate or Subscriber, a report must include at least one of the following:

- the Certificate serial number; or
- GlobalSign order number; or
- FQDN; or
- Subject information; or
- CT log information (e.g link to crt.sh).

For the information to verify the details of the claims made in the Certificate Problem Report, these must include the following information:

- For reports of Key Compromise: proof of the compromise, in the form of a link to the location where the Private Key can be found or a signed CSR which includes an indication that the key has been compromised (e.g. “CSR for Compromised Key” in the common name field).
- For malware, phishing or fraudulent use reports: description of the malicious behaviour and a link to tools that offer analysis of submitted code (e.g. Virus Total) or the contents of websites (e.g. Google Safe Browsing).

If insufficient information is provided, GlobalSign may request additional information in the preliminary report on its findings and will further action the Certificate Problem Report once all relevant information has been provided.

GlobalSign records if the Certificate Problem Report cannot be confirmed, the actions taken along with the justification. The timeline for revocation as stated in Section 4.9.1. starts from the moment all relevant information has been confirmed.

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 to request revocation of a suspected Key Compromise, use of a weak key or

discovery of inaccurate information within an issued Certificate. A risk analysis shall be completed and recorded for any revocations that cannot be processed by either party for any reason.

Subscribers have 48 hours to inform GlobalSign of a Key Compromise.

4.9.5. Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, GlobalSign investigates the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

For Mark Certificates, within a commercially reasonable period of time sufficient to confirm all relevant facts and communicate with all relevant parties, GlobalSign investigates the facts and circumstances related to a Court Order of Infringement submitted by a Conflicting Trademark Owner and thereafter provides appropriate notice and takes appropriate action.

After reviewing the facts and circumstances, GlobalSign works with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which the CA will revoke the Certificate.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.

For the date of revocation, GlobalSign considers at least the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn’t receive the goods they ordered); and
5. Relevant legislation.

GlobalSign considers a Certificate Problem Report to be received when the Certificate Problem Report is supported by sufficient information to allow GlobalSign to identify the reported Certificate or specific Subscriber, and to verify the details of the claims in line with Section 4.9.3.1.

All revocation requests for end entity Certificates generated via the Subscriber account are processed within a maximum of 24 hours of receipt.

4.9.5.1. Code Signing Certificates

GlobalSign maintains a continuous 24x7 ability to communicate with Anti-Malware Organizations, Application Software Suppliers, and law enforcement agencies and respond to high-priority Certificate Problem Reports, such as reports requesting revocation of Certificates used to sign malicious code, fraud, or other illegal conduct.

GlobalSign acknowledges receipt of plausible notices about Suspect Code signed with a Certificate issued by GlobalSign or one of its Subordinate CAs.

GlobalSign begins investigating Certificate Problem Reports within twenty-four hours of receipt, and decides whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem (adware, spyware, malware, software bug, etc.);
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the report (for example, a notification from an Anti-Malware Organization or law enforcement agency carries more weight than an anonymous complaint); and
4. Relevant legislation.

4.9.6. Revocation Checking Requirements for Relying Parties

Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate for the intended purpose and ensure the Certificate is valid, otherwise all warranties become void.

Relying Parties will need to consult the 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). For Qualified Certificates, validation of the Certificate chain must be carried out successfully up to the GlobalSign trust anchor within the EU trusted list.

Relying Parties should note that because CRLs are issued at set time frames there may be a period directly after revocation and before next CRL generation where OCSP and CRL do not return the same status. In cases where differences between CRL and OCSP occur, OCSP should be presumed to be most accurate.

GlobalSign includes applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process.

4.9.7. CRL Issuance Frequency

For CAs which issue Publicly-Trusted TLS Certificates, CRLs will be generated and published within 24 hours of first Certificate issuance.

For CAs issuing Subscriber Certificates with CRLs:

- GlobalSign updates and publishes a new CRL at least every:
  1. seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod (“AIA OCSP pointer”); or
  2. four (4) days in all other cases;
- GlobalSign updates and publishes a new CRL within twenty-four (24) hours after recording a Certificate as revoked; and
- The value of the nextUpdate field will not be more than ten days beyond the value of the thisUpdate field.

For CAs issuing Qualified Certificates:

- GlobalSign updates and publishes a new CRL at least every twenty-four (24) hours.

For CAs issuing CA Certificates:

- GlobalSign updates and publishes a new CRL at least every twelve (12) months; and
- GlobalSign updates and publishes a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

GlobalSign continues issuing CRLs until one of the following is true:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; or
- the corresponding Subordinate CA Private Key is destroyed.

For the status of Timestamp Certificates:

GlobalSign updates and reissues CRLs at least once every twelve months and within 24 hours after revoking a Timestamp Certificate, and the value of the nextUpdate field will 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

GlobalSign OCSP responses conform to RFC6960 and/or RFC5019.

OCSP Responders operated by GlobalSign 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 have a validity interval greater than or equal to eight hours;
2. OCSP responses have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, GlobalSign updates 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, GlobalSign updates 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 Publicly-Trusted TLS Certificates, an authoritative OCSP response is available (i.e. the responder does not respond with the "unknown" status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.

For the status of Subordinate CA Certificates:

- GlobalSign updates information provided via an OCSP Responder at least every twelve months and within 24 hours after revoking a Subordinate CA Certificate.

For the status of Timestamp Certificates:

- If the Subordinate CA provides OCSP responses, the Subordinate CA updates information provided via an OCSP response at least every twelve months and within 24 hours after revoking a Timestamp Certificate.

OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a “good” status for such Certificates.

OCSP Responders for CAs which are not Technically Constrained, in line with Section 7.1.5, will not respond with a “good” status for such Certificates.

OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. Each OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-Line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

GlobalSign and any of its 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 GlobalSign at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, GlobalSign shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRLs within 30 minutes of creation and ARLs within 12 hours.

Where Key Compromise occurs on CA Certificates on the EU eIDAS trusted list, GlobalSign will inform the applicable Supervisory Body to withdraw the CAs from the applicable trusted list.

Parties may use the following methods to demonstrate Key Compromise:

- Submission of a CSR file, created and signed by the Private Key. The CSR file needs to contain one of the

following:

- A specific string that GlobalSign has provided to the reporter.
  OR
- A string of text that clearly indicates compromise.

- Providing references to vulnerability and/or security incident sources from which the Compromise is verifiable
- Submission of binaries that contain a Compromised Private Key, including the method to extract the Private Key

GlobalSign will analyze other requests and update the CPS accordingly if the new method of submission is accepted.

4.9.13. Circumstances for Suspension

Certificate suspension is available for EPKI customers. Certificate suspension can be used when an EPKI administrator wants to disable client Certificates temporarily. Such situations may include temporary loss of Certificates and temporary leave of users from organization, etc. Unlike Certificate revocation which disables a Certificate permanently, Certificate suspension status can be lifted by an EPKI administrator to reactivate the Certificate.

Certificate suspension is not supported for SSL, Code Signing, timestamping, Qualified, S/MIME BR (strict profile) or Mark Certificates.

4.9.14. Who Can Request Suspension

EPKI administrators can request suspension and lifting of Certificate suspension through GCC. GlobalSign does not process Certificate suspension unless requested through GCC.

4.9.15. Procedure for Suspension Request

EPKI administrators can request Certificate suspension in GCC. After the request is submitted in GCC, such information is synchronized with RA and CA to process the suspension request. Certificate suspension is listed in the CRL with reason code of “certificateHold.”

4.9.16. Limits on Suspension Period

Certificate suspension may last as long as the validity period of Certificate.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

GlobalSign provides a Certificate status service in the form of an OCSP Responder and/or a CRL distribution point. The integrity and authenticity of this status information is secured and protected.

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, GlobalSign does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

Except for the case of suspension, the revocation status will never be reverted.

If required by Root Programs or CA/B Forum requirements, GlobalSign 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.

GlobalSign may backdate revocation for Code Signing Certificates. Where GlobalSign backdates revocation for Code Signing, GlobalSign shall as an exception to best practice described in RFC 5280 follow the Baseline Requirements for Code Signing recommendation to use revocationDate instead of invalidityDate within its CRL.

4.10.2. Service Availability

GlobalSign operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. GlobalSign maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by GlobalSign.

GlobalSign maintains 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.

Upon system failure, service or other factors which are not under the control of GlobalSign, GlobalSign aims to ensure that this information service is not unavailable for longer than 24 hours.

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.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

CA Private Keys are not escrowed. GlobalSign does not offer key escrow services to Subscribers.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

GlobalSign has developed, implemented, and maintains 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 includes:

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.

GlobalSign's security program includes 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, GlobalSign has developed, implemented, and maintains 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 includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements 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

5.1.1. Site Location and Construction

GlobalSign's CAs are located within secure data centers. The data centers are purpose-built facilities.

5.1.2. Physical Access

GlobalSign's CAs are operated within secure data centers that provide on-premise security with biometric scanners, card access systems and multiple barriers and security check points prior to entry. A 24x7 Closed Circuit TV (CCTV) monitoring system as well as digital recording is provided. Security guards secure the physical premises and only security-cleared and authorized personnel are allowed onto the premises.

5.1.3. Power and Air Conditioning

GlobalSign's CAs are operated within secure data centers that are equipped with redundant power and cooling systems. UPS and power generators are in place to ensure continuity in the unlikely event of power outage.

5.1.4. Water Exposures

GlobalSign's CAs are protected against water. They are located above ground and on a higher floor with raised flooring. In addition, a water detection alarm system is in place, and on-site data center operations staff are ready to respond to any unlikely water exposure.

5.1.5. Fire Prevention and Protection

GlobalSign's CAs operate within secure data centers that are equipped with a fire detection and suppression system.

5.1.6. Media Storage

Storage of backup media is performed both on- and off-site and is physically secured and protected from fire and water damage.

5.1.7. Waste Disposal

GlobalSign ensures that all media used for the storage of information is declassified or securely destroyed before being released for disposal.

5.1.8. Off-Site Backup

As stipulated in Section 5.5.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles are free from conflict of interest that might prejudice the impartiality of GlobalSign's operations.

Trusted roles include, but are not limited to, members of the following teams:

- Security, Compliance and Privacy
- Validation Specialists
- Key management
- Infrastructure
- Auditors

5.2.2. Number of Persons Required per Task

CA Private Keys are backed up, stored, and recovered only by a quorum of trusted role personnel, using, at least, dual control in a physically secured environment.

5.2.3. Identification and Authentication for Each Role

Before appointing a person to a trusted role, a background check is performed.

Trusted roles must identify and authenticate themselves prior to accessing GlobalSign's systems.

5.2.4. Roles Requiring Separation of Duties

CA personnel are specifically assigned 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;
- Those performing installation, configuration, and maintenance of the CA systems;
- Those with overall responsibility for administering the implementation of the CA's security practices;
- Those performing duties related to cryptographic key life cycle management;
- Those performing CA systems development; and
- Those performing CA systems auditing.

GlobalSign enforces rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. These control procedures are auditable.

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, GlobalSign verifies the identity and trustworthiness of such person.

Personnel must demonstrate expert knowledge, experience, and qualifications as appropriate to the job function. Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions.

Job descriptions are defined from the viewpoint of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. GlobalSign personnel are formally appointed to Trusted Roles.

5.3.2. Background Check Procedures

All GlobalSign personnel in Trusted Roles are free from conflict of interests that might prejudice the impartiality of the CA operations. GlobalSign does not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence if 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 analyzed, 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 where permitted by law.

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

5.3.3. Training Requirements

GlobalSign provides all personnel performing information verification duties with skills training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this document), common threats to the information verification process (including phishing and other social engineering tactics), and the applicable Industry Standards.

GlobalSign maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. GlobalSign documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

GlobalSign requires all Validation Specialists to pass an examination provided by the CA on the Information verification requirements outlined in the applicable Industry Standards.

If a Validation Specialist is to be engaged in the EV Processes, the required internal examination relates to the EV Certificate validation criteria outlined in the EV Guidelines.

5.3.4. Retraining Frequency and Requirements

All personnel in Trusted Roles maintain skill levels consistent with GlobalSign's annual training and performance programs with relevance to their trusted role.

GlobalSign provides information security and privacy training at least once a year to all personnel.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

A process is in place to apply appropriate disciplinary sanctions to personnel violating GlobalSign's operational procedures and policies.

5.3.7. Independent Contractor Requirements

GlobalSign verifies 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.

5.3.8. Documentation Supplied to Personnel

GlobalSign makes available to its personnel this document, and any relevant statutes, policies, or contracts.

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

GlobalSign and Delegated Third Parties record events related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems. GlobalSign and Delegated Third Parties 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. GlobalSign makes these records available to its Qualified Auditor.

GlobalSign records at least the following events:

CA Certificate and key lifecycle events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Certificate requests, renewal, and re-key requests, and revocation;

- Approval and rejection of Certificate requests;
- Cryptographic device life cycle management events
- Generation of Certificate Revocation Lists and OCSP entries;
- Signing of OCSP Responses; and
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles;

Subscriber Certificate life cycle management events, including:

- Certificate requests, renewal, and re-key requests, suspension and revocation;
- All verification activities stipulated in this document;
- Approval and rejection of Certificate Requests;
- Issuance of Certificates;
- Generation of Certificate Revocation Lists, and
- Signing of OCSP Responses;

Security events, including:

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

Log records 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

Audit logs are reviewed on an as needed basis.

5.4.3. Retention Period for Audit Log

GlobalSign and Delegated Third Parties 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)(1) after the later

occurrence of:

1. the destruction of the CA Private Key; or
2. 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)(2) after the revocation or expiration of the Subscriber Certificate; and
3. Any security event records (as set forth in Section 5.4.1.1(3)

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

5.4.4. Protection of Audit Log

Events are 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 records of events are protected to prevent alteration and detect tampering and to ensure that only individuals with authorized access are able to perform any operations without modifying integrity, authenticity, and confidentiality of the data.

The records of events are 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 realization.

5.4.5. Audit Log Backup Procedures

Audit logs are regularly backed-up in a secure location. The logs are protected with at least the same level of security as the original logs.

5.4.6. Audit Collection System

Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects the data confidentiality. In case of a problem occurring during the process of the audit collection GlobalSign determines whether to suspend GlobalSign operations until the problem is resolved.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

GlobalSign performs at least an annual risk assessment that:

- 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;

- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

GlobalSign also performs regular vulnerability assessments and penetration tests covering GlobalSign assets related to Certificate issuance, products, and services. Assessments focus on internal and external threats which 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

GlobalSign and Delegated Third Parties archive all audit logs as set forth in Section 5.4.1 and:

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) are 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, GlobalSign and Delegated Third Parties 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)
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

Archives are protected throughout their lifetime using both physical and logical access controls to protect against unauthorized modification or destruction.

5.5.4. Archive Backup Procedures

Backups of archived data are made on a regular basis.

5.5.5. Requirements for Timestamping of Records

GlobalSign timestamps all logs indicating the time at which the event occurred.

5.5.6. Archive Collection System (Internal or External)

No stipulation.

5.5.7. Procedures to Obtain and Verify Archive Information

No stipulation.

5.6. Key Changeover

Before expiration of a CA Certificate, GlobalSign may periodically changeover key material for Issuing CAs in accordance with Section 6.3.2.

Certificate Subject information may also be modified, and Certificate profiles may be altered to adhere to 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

5.7.1.1. Incident Response and Disaster Recovery Plans

GlobalSign documents business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

The business continuity plan includes:

- The conditions for activating the plan,
- Emergency procedures;
- Fallback procedures;
- Resumption procedures;
- A maintenance schedule for the plan;

- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery time objective (RTO);
- Regular testing of contingency plans;
- GlobalSign's plan to maintain or restore GlobalSign's business operations in a timely manner following interruption to or failure of critical business processes;
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- What constitutes an acceptable system outage and recovery time;
- How frequently backup copies of essential business information and software are taken;
- The distance of recovery facilities to the CA's main site; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

GlobalSign tests, reviews and updates these procedures annually.

5.7.1.2. Mass Revocation Plans

GlobalSign maintains a comprehensive and actionable plan for mass revocation events, performs annual testing of this plan, and incorporates lessons learned to continually improve preparedness for mass revocation events over time.

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 GlobalSign's disaster recovery plan.

5.7.3. Entity Private Key Compromise procedures

In the event a GlobalSign CA Private Key is Compromised, lost, destroyed, or suspected to be Compromised, GlobalSign, after investigation of the problem, shall decide if the CA Certificate should be revoked.

Upon confirmation of the Compromise:

- All the Subscribers who have been issued a Certificate from this hierarchy will be notified at the earliest feasible opportunity
- Revocation status information will be provided and maintained at a publicly accessible location in case of CA Key Compromise, including, if applicable, transferring Certificate status information services to another GlobalSign group entity.
- Prompt notification of the compromise shall be provided to Relying Parties, including details that Certificates and revocation status information issued using the compromised CA key may no longer be valid

- A new CA Private Key and Certificate shall be generated, or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.
- If a new CA has been created, the CA Public Key shall be published on the public repository.

5.7.4. Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with business continuity capabilities as described in Section 5.7.1.

5.8. CA or RA Termination

In case of termination of CA or RA activities, the impact of the termination will be minimized as much as possible in light of the prevailing circumstances.

The procedures to be followed must, at a minimum:

- ensure that any disruption caused by the termination of an Issuing CA is minimized as much as possible;
- ensure that archived records of the Issuing CA are retained;
- ensure that prompt notification of termination is provided to Subscribers, Authorized 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 GlobalSign group entity;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained;
- notify auditors; and
- notify other relevant Government and Certification bodies under applicable laws and related regulations.

For Code Signing/Timestamp Certificates: give 90 days' prior notice to all Application Software Suppliers relying on the Root Certificate and permit the Application Software Suppliers sufficient time to take appropriate action as determined by the Application Software Supplier.

5.8.1. Successor Certification Authority

To the extent that it is practical and reasonable, any appointed successor CA should:

- Issue new Certificates to all impacted Subscribers
- Assume the same rights, obligations and duties as the terminating CA.

6. 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 performs 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, GlobalSign also performs 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;
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

Code Signing

GlobalSign generates and protects Private Keys associated with its Root CA Certificates and new Subordinate CA Certificates used for signing TSU keys for Code Signing and Extended Validation Code Signing with a validity period of greater than 72 months containing the id-kp-timeStamping KeyPurposeId in the extKeyUsage extension in a Hardware Crypto Module conforming to the requirements specified in Baseline Requirements for Code Signing Section 6.2.7.1, maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

For Publicly-Trusted Code Signing, TLS, S/MIME and Mark Certificates:

GlobalSign will reject a Certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. GlobalSign is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. GlobalSign has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1; or
5. GlobalSign is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak keys).

GlobalSign does not generate Private Keys for Publicly-Trusted TLS or Code Signing Certificates.

For Subscriber keys generated by GlobalSign, Key generation is performed:

- within 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; and
- in accordance with the Industry Standards (where applicable).

Code Signing Certificates

Keys 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+.

6.1.2. Private Key Delivery to Subscriber

GlobalSign CAs that create Private Keys on behalf of Subscribers do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber.

For non-Publicly-Trusted TLS Certificates, this is achieved through the use of PKCS#12 (.pfx) files containing Private Keys and Certificates encrypted by at least sixteen (16) character password. At least eight (8) characters are system generated and provided to the Subscriber during the enrolment process and the Subscriber specifies at least eight (8) characters. For S/MIME Certificates, this is again achieved through the use of PKCS#12 (.pfx) files containing Private Keys and Certificates encrypted by a minimum seventeen (17) alpha-numeric character Subscriber-selected password.

GlobalSign ensures the integrity of any Public/Private Keys and the randomness of the key material through a suitable RNG or PRNG. If GlobalSign detects or suspects that the Private Key has been communicated to an unauthorized person or an organization not Affiliated with the Subscriber, then GlobalSign revokes all Certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3. Public Key Delivery to Certificate Issuer

GlobalSign CAs 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

GlobalSign ensures that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks. Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys into their root stores and operating systems. Issuing CA Public Keys are delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by GlobalSign and referenced within the profile of the issued Certificate through AIA (Authority Information Access).

6.1.5. Key Sizes

Key Pairs generated by GlobalSign conform to the following characteristics:

For RSA Key Pairs:

- The modulus size, when encoded, is at least 2048 bits
- The modulus size, in bits, is evenly divisible by 8.

For ECDSA Key Pairs:

- The key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

6.1.5.1. AATL

The minimum key size for Root CAs is RSA 3072-bit or ECC NIST P-384.

6.1.5.2. Code Signing

For Key Pairs corresponding to Root and Subordinate CAs:

- If the Key is RSA, then the modulus MUST be at least 4096 bits in length.
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.

For Key Pairs corresponding to Subscriber code signing and Timestamp Authority Certificates:

- If the Key Pair is RSA, then the modulus MUST be at least 3072 bits in length.
- If the Key Pair is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.

6.1.5.3. Qualified Certificates for Website Authentication

For RSA Key Pairs:

- The modulus size, when encoded, is at least 3072 bits.

6.1.6. Public Key Parameters Generation and Quality Checking

RSA: GlobalSign confirms that the value of the public exponent is an odd number equal to 3 or more and that the public exponent should be in the range between 2^16 + 1 and 2^256 - 1.

GlobalSign also checks that the modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: GlobalSign may confirm the validity of all keys using either the ECC Full Public Key

Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

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

GlobalSign sets 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 are not used to sign Certificates except as permitted by Section 6.1.7 of the applicable CA/Browser Forum and MC Requirements.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

GlobalSign implements physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified in Section 6.2.7 consists of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key.

Private Keys are encrypted 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

6.2.1.1. CA Private Key Standards and Controls

GlobalSign protects its CA Private Keys 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.

6.2.1.2. Timestamp Authority Private Key Standards and Controls

Private Keys of Timestamp Authorities are protected 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+ (ALC_FLR.2), or higher.

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

CA Private Keys for cryptographic operations are activated 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

GlobalSign does not escrow Private Keys for any reason.

6.2.4. Private Key Backup

Root CA and Subordinate CA Private Keys are backed up, stored, and recovered only by personnel in Trusted Roles using, at least, dual control in a physically secured environment.

6.2.5. Private Key Archival

GlobalSign does not archive CA Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

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

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

6.2.7. Private Key Storage on Cryptographic Module

GlobalSign stores CA Private Keys on a device meeting the requirements of Section 6.2.1.

6.2.8. Method of Activating Private Key

GlobalSign activates CA Private Keys 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

GlobalSign deactivates CA Private Keys in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module.

6.2.9.1. Code Signing

Private Keys associated with Code Signing and Extended Validation Code Signing Timestamp Certificates issued for greater than 15 months are removed from the Hardware Crypto Module protecting the Private Key within 18 months after issuance of the Timestamp Certificate.

For Timestamp Certificates for Code Signing and Extended Validation Code Signing issued on or after June 1, 2024, GlobalSign logs the removal of the Private Key from the Hardware Crypto Module through means of a key deletion ceremony, witnessed and signed-off by at least two Trusted Role members. GlobalSign may also perform a key destruction ceremony, meaning that all copies of that Private Key are unequivocally/securely destroyed (i.e. without a way to recover the key), including any instance of the key as part of a backup, to satisfy this requirement.

6.2.10. Method of Destroying Private Key

GlobalSign destroys CA Private Keys in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module.

The CA Private Keys residing on the Hardware Security Module shall be destroyed upon device retirement.

Note: This destruction does not necessarily affect all copies of the Private Key. Only the physical instance of the key stored in the secure cryptographic device under consideration will be destroyed.

6.2.11. Cryptographic Module Rating

See Section 6.2.1

6.3. Other Aspects of Key Pair Management

GlobalSign shall not use its CA private signing keys beyond the end of their life cycle. CA signing key(s) used for generating Certificates and/or issuing revocation status information, shall not be used for any other purpose. The use of CA Private Keys shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating Certificates in line with current best practice.

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1. Root and Issuing CAs

Certificates have a maximum Validity Period of:

Type	Key Pair Usage Period	Max Validity Period
Root Certificates	No stipulation	25 years
TPM Root Certificates	30 years	41 years
Publicly Trusted Sub-CAs/Issuer CAs	No stipulation	18 years

6.3.2.2. Subscriber Certificates

Type	Key Pair Usage Period	Max Validity Period
PersonalSign Certificates	No stipulation	39 months
Code Signing Certificates	No stipulation	460 days
EV Code Signing Certificates	No stipulation	460 days
S/MIME strict and multipurpose Certificates	No stipulation	825 days
AATL End Entity Certificates	No stipulation	39 months
DV SSL Certificates	No stipulation	200 days
AlphaSSL Certificates	No stipulation	200 days
OV SSL Certificates	No stipulation	200 days
EV SSL Certificates	No stipulation	200 days
Qualified Website Authentication Certificates	No stipulation	200 days
Mark 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

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.

For Mark Certificates, the validity period shall not exceed the period defined in Section 6.3.2 of the MC Requirements.

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.

GlobalSign complies with the Industry Standards with respect to the maximum Validity Period.

In the event that a Subscriber's Certificate has a reduced validity period, subsequent re-issues may be used to regain that lost validity period.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Activation data for CA Private Keys is generated during a key ceremony in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module.

It is then delivered to a holder of a share of the data who is a person in a trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2. Activation Data Protection

CA Private Key activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms.

6.4.3. Other Aspects of Activation Data

CA Private Key activation data may only be held by GlobalSign personnel in Trusted Roles.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The following security functions are provided through a combination operating system and software controls:

- Systems performing CA functions are not used for general purposes
- Strong password policies are implemented
- Inactive lockouts are implemented
- Security patches are reviewed, tested and timely applied
- Authenticated logins for Trusted Roles
- Access control with least privilege
- Means for malicious code detection and protection
- Security audit capability, protected in integrity.

Multi-factor authentication is required for all accounts capable of directly causing Certificate issuance.

6.5.2. Computer Security Rating

No stipulation.

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

System development controls for CA systems are as follows:

- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. Commercial off-the-shelf hardware and software must meet minimum security and quality levels and is subject to a vendor selection process;
- Hardware will be inspected during the commissioning process to ensure conformity of the supplied hardware, and to confirm the hardware has not been tampered with. Hardware and software procured are procured using controls to reduce the likelihood of tampering;
- 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 operations;
- 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. Hardware and software are scanned for malicious code;
- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and approved personnel in a defined manner; and
- Hardware will be monitored to ensure it is functioning correctly.

6.6.2. Security Management Controls

The configuration of GlobalSign CA systems as well as any modifications and upgrades are documented and controlled. There is an automatic mechanism for detecting unauthorized modification to GlobalSign software or configuration. This includes checking whether changes violate GlobalSign security policies. Where applicable, manual configuration reviews are performed on at least an annual basis. A formal configuration management methodology is used for installation and on-going maintenance of GlobalSign CA systems. Software, when first loaded, is checked as being supplied from the vendor, with no modifications, and to confirm if it is the version intended for use.

6.6.3. Lifecycle Security Controls

Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.

6.7. Network Security Controls

GlobalSign implements security measures in accordance with the CA/Browser Forum's Network and Certificate System Security Requirements to ensure:

- Certificate Systems are segmented into networks based on their functional or logical relationship;
- Equivalent security controls are applied to all systems co-located in the same network with a Certificate System; and
- Each network boundary control is configured with rules that support only the services, protocols, ports, and communications that GlobalSign has identified as necessary to its operations.

Vulnerabilities are documented, reviewed and remediated based on risk assessment and security analysis. Critical vulnerabilities are assessed within 48 hours, high and medium risk vulnerabilities are remediated within 30 to 90 days.

6.8. Timestamping

GlobalSign infrastructure is synchronized with UTC at least once every 24 hours.

6.8.1. PDF Signing Timestamping Services

All Digital Signatures created by PDF Signing Certificates have the ability to include a trusted timestamp issued from an RFC 3161 compliant Time Stamp Authority (TSA) server chained to a GlobalSign Root Certificate. The TSA Certificate shall be located in a FIPS 140-2 level 3 or higher HSM.

6.8.2. Code Signing and EV Code Signing Timestamping Services

All Digital Signatures created by Code Signing and Extended Validation Code Signing Certificates have the ability to include a trusted timestamp issued from an RFC 3161 compliant Time Stamp Authority (TSA) server chained to a GlobalSign Root Certificate. The TSA Certificate shall be located in a FIPS 140-2 level 3 or higher HSM.

Timestamp Certificates for Code Signing and Extended Validation Code Signing issued on or after April 15, 2025, issued by a Timestamp Authority Subordinate CA with a validity period greater than 72 months, will be signed by a Private Key generated and protected in a Hardware Crypto Module conforming to the requirements specified in Baseline Requirements for Code Signing Section 6.2.7.1, maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

GlobalSign issues Certificates in compliance with RFC 5280 and the applicable Industry Standards except as otherwise specified in this document.

7.1.1. Version Number(s)

GlobalSign issues Certificates in compliance with X.509 Version 3.

7.1.2. Certificate Extensions

Criticality follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

Subordinate CA and end entity Certificates include an Extended Key Usage extension containing KeyPurposeId(s) describing the intended usage(s) of the Certificate. The KeyPurposeId anyExtendedKeyUsage is not included in Publicly-Trusted end entity Certificates.

The following Extensions may additionally be included in End Entity Certificates:

- privateKeyUsagePeriod within Certificates for timestamping
- Qualified Certificate Statements within Qualified Certificates
- microsoftCertTemplateV2
- logotype within Mark Certificates
- Pilot identifier within Mark Certificates

Other Extensions may additionally be included in End Entity Certificates at customer request after evaluation by GlobalSign.

7.1.3. Algorithm Object Identifiers

GlobalSign issues 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

GlobalSign uses signature algorithms and encodings in line with Section 7.1.3 of the applicable CA/Browser Forum and MC Requirements.

7.1.4. Name Forms

GlobalSign issues Certificates with name forms compliant to RFC 5280 and Section 7.1.4 of the applicable CA/Browser Forum and MC Requirements. Included attributes are validated in accordance with Section 7.1.4.2 of the applicable CA/Browser Forum and MC Requirements.

S/MIME Certificates may include a user principal name (UPN) in the otherName entry within the subjectAltName extension and a szOID_Certificate_TEMPLATE extension (Microsoft Open Specifications).

OCSP Responder Certificates may include a subject serialNumber attribute to fulfil DN uniqueness requirements.

For a Qualified Website Authentication CA Certificate, the subject field may contain the attribute organizationIdentifier. GlobalSign includes this information where an appropriate registration number is known to exist for the issuer and this information is required following WEB-4.1.2-3 in ETSI EN 319 412-4. The validation happens following the Organization Identifier validation process for Subscriber Certificates.

7.1.5. Name Constraints

GlobalSign may issue Subordinate CA Certificates with name constraints where permitted by Section 7.1.5 of the applicable CA/Browser Forum Requirements.

GlobalSign does not include the nameConstraints extension in Mark Certificate hierarchies.

7.1.6. Certificate Policy Object Identifier

GlobalSign applies the following requirements:

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

Certificate type	Source	Section
Mark	MC Requirements	7.1.6

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

GlobalSign issues Certificates with a policy qualifier and may include suitable text to aid Relying Parties in determining applicability.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.1.10. Serial Numbers

Each Issuing CA must issue Certificates that include a unique (within the context of the Issuer Subject DN and CA Certificate serial number) non-sequential Certificate serial number greater than zero (0) containing at least 64 bits of output from a CSPRNG.

As an exception to RFC5280 in TLS Certificates, a TLS Precertificate and Certificate share the same serialNumber value.

7.1.11. Special Provisions for Qualified Certificates

Qualified Certificates are configured to meet the applicable profile requirements of ETSI EN 319 412 and ETSI TS 119 495.

7.1.11.1. Qualified Web Authentication Certificates

Qualified Web Authentication Certificates contain the following qualified statements:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-web

Qualified Web Authentication Certificates which are issued for Open Banking include “id-etsi-psd2-qcStatement”.

7.2. CRL Profile

7.2.1. Version Number(s)

GlobalSign issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:

- **Issuer** The Subject DN of the issuing CA
- **Effective date** Date and Time
- **Next update** Date and Time
- **Signature Algorithm** sha256RSA etc. (Depending upon product)
- **Signature Hash Algorithm** sha256 etc. (Depending upon product)
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

7.2.2. CRL and CRL Entry Extensions

CRLs have the following extensions:

- **CRL Number** Monotonically increasing serial number for each CRL
- **Authority Key Identifier** AKI of the issuing CA for chaining/validation requirements

Following extensions are supported:

- **ReasonCode** Identifies the reason for the Certificate revocation.

The extension is present for a CRL entry for a Root CA or Subordinate CA Certificate, including Cross Certificates. Supported values are keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5), privilegeWithdrawn (9).

The extension may be present for a CRL entry for a Subscriber end entity Certificate. Supported values are keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6), privilegeWithdrawn (9).

The value certificateHold (6) not supported for SSL, Code Signing, timestamping, Qualified, S/MIME BR (strict profile) or Mark Certificates.

7.3. OCSP Profile

GlobalSign operates an Online Certificate Status Protocol (OCSP) responder in compliance with RFC 6960 and RFC 5019 and highlights this within the AIA extension via an OCSP Responder URL.

7.3.1. Version Number(s)

GlobalSign issues Version 1 OCSP responses with following fields:

- Responder ID SHA-1 Hash of responder’s Public Key
- Produced Time The time at which this response was signed
- Certificate Status Certificate status referenced (good/revoked/unknown)
- ThisUpdate/NextUpdate Recommended validity interval for the response
- Signature Algorithm SHA256 RSA etc. (depending upon product)
- Signature Signature value generated by the responder
- Certificates The OCSP Responder’s Certificate

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

Following fields are supported:

- revocationReason Identifies the reason for the Certificate revocation.

This field is present for OCSP responses for a Root CA or Subordinate CA Certificate, including Cross Certificates, and may be present for a Subscriber end entity Certificate, if the Certificate is revoked. The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.2. OCSP Extensions

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessments

The procedures within this document are designed to comply with the requirements listed in Section 1.0 and encompass all relevant portions of currently applicable Industry Standards.

GlobalSign undergoes audits in accordance with Section 8.0 of the applicable CA/Browser Forum and MC Requirements, and where applicable, the requirements identified in Section 1.0.

8.1. Frequency and Circumstances of Assessment

GlobalSign maintains its compliance with the WebTrust/eIDAS standards identified in Section 1.0 via a Qualified Auditor on an annual basis.

8.2. Identity/Qualifications of Assessor

The audit of GlobalSign is performed by a “Qualified Auditor” that possesses the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in Section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
- Bound by law, government regulation, or professional code of ethics; and
- Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million ($1,000,000) US dollars in coverage, except in the case of an internal government auditing agency (this exception is not applicable to Mark Certificates).

For eIDAS, the audit is 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

GlobalSign selects an auditor/assessor who is completely independent from GlobalSign.

8.4. Topics Covered by Assessment

The audit meets the requirements of the audit schemes highlighted in Section 1.0 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

GlobalSign, including cross-signed Issuing CAs that are not technically constrained, follow the same process if presented with a material non-compliance by auditors and create a suitable corrective action plan to remove the deficiency. Corrective action plans which directly affect policy and procedure as dictated by the CP and CPS are referred to the GlobalSign policy authority.

8.6. Communications of Results

Results of the audit are reported to the 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

GlobalSign monitors its adherence to this document and Industry Standards and strictly controls 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 Certificates) of the Certificates issued during the period commencing immediately after the previous self-audit sample was taken.

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, GlobalSign will ensure the practices and procedures of delegated parties are in compliance with the applicable Industry Standards and the relevant CP and/or CPS. GlobalSign documents the obligations of delegated parties and performs monitoring on at least an annual basis of the delegated parties' adherence with those obligations.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

GlobalSign charges fees for Certificate issuance and renewal. GlobalSign does not charge for reissuance. Fees and any associated terms and conditions are made clear to Applicants both by the enrollment process through a web interface or in the sales and marketing materials on GlobalSign's various language specific web sites.

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

GlobalSign 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 GlobalSign's Certificate status infrastructure.

9.1.4. Fees for Other Services

GlobalSign may charge for other additional services such as timestamping.

9.1.5. Refund Policy

For customers who have a direct relationship with GlobalSign and Certificates ordered directly from GlobalSign, if a Subscriber is not completely satisfied with the issued Certificate, the Subscriber may request a refund within 7 days of the Certificate being issued. Any refunds will be net of any fees incurred by GlobalSign.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

GlobalSign NV/SA maintains 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 US dollars ($5,000,000) in coverage. GlobalSign'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

GlobalSign offers a Warranty Policy to Subscribers published on GlobalSign's website at https://www.globalsign.com/en/company/corporate-policies.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by GlobalSign:

- Personal Information as detailed in Section 9.4;
- Audit logs from CA and RA systems;
- Activation data used to activate CA Private Keys as detailed in Section 6.4;
- Internal GlobalSign business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and
- Audit Reports from an independent auditor as detailed in Section 8.0.

9.3.2. Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3. Responsibility to Protect Confidential Information

GlobalSign protects confidential information through training and enforcement with employees, agents, and contractors.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

GlobalSign protects personal information in accordance with a Privacy Policy published on GlobalSign's website at https://www.globalsign.com/repository.

9.4.2. Information Treated as Private

GlobalSign treats 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 and applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected.

GlobalSign periodically trains anyone who has access to the information about due care and attention that must be applied.

9.4.3. Information Not Deemed Private

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

9.4.4. Responsibility to Protect Private Information

GlobalSign is responsible for securely storing private information in accordance with a published Privacy Policy document and may store information received in either paper or digital form. GlobalSign protects private information using appropriate safeguards and a reasonable degree of care and requires the same from any service providers handling private information on behalf of GlobalSign or an RA.

9.4.5. Notice and Consent to Use Private Information

Personal information obtained from Applicants during the application and enrollment process is deemed private and permission is required from the Applicant to allow the use of such information. GlobalSign includes any required consents in the Subscriber Agreement, including any permission required for additional information to be obtained from third parties that may be applicable to the validation process for the product or service being offered by GlobalSign.

GlobalSign requires the same from any service providers who handle private information on behalf of GlobalSign or an RA.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

GlobalSign 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

GlobalSign does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. GlobalSign retains ownership of Certificates; however, it grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

GlobalSign and the GlobalSign logo are the registered trademarks of GMO GlobalSign K.K.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

GlobalSign uses this document and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties.

By issuing a Certificate, GlobalSign 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.

GlobalSign represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid, the Issuing CA has complied with this document in issuing and managing the Certificate.

9.6.1.1. General representations and warranties

For SSL, EV SSL, S/MIME, Code Signing, EV Code Signing and Mark Certificates, GlobalSign represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid, GlobalSign has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate and:

- **Right to Use Domain Name or IP Address**: For SSL and Mark Certificates, that, at the time of issuance, GlobalSign (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP Address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Right to Use Mailbox Address**: For S/MIME Certificates, that, at the time of issuance, GlobalSign (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses listed in the Certificate's subject field and subjectAltName extension (or was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and iii. accurately described the procedure in GlobalSign's CP and/or CPS (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, GlobalSign (i) operated a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, GlobalSign (i) operated a procedure for verifying all of

the information contained in the Certificate (with the exception of the subject:organizationalUnitName and subject:serialNumber (non-EV Certificates) attribute) was true and accurate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.2, 3.2.3, 3.2.4);

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, GlobalSign (i) operated a procedure to verify the identity of the Applicant in accordance with Section 3.2 and Section 7 of the applicable CA/Browser Forum and MC Requirements; (ii) followed the procedure when issuing and managing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.2, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if GlobalSign and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the applicable CA/Browser Forum and MC Requirements or, if GlobalSign and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.1);
- **Status:** That GlobalSign maintains a 24 x 7 publicly accessible Repository with current information regarding the status of Certificates as valid or revoked for the period required by the applicable Industry Standards; and
- **Revocation:** That GlobalSign will revoke the Certificate for any of the reasons specified in the applicable Industry Standards (see Section 4.9.1).

9.6.1.2. Representations and warranties for Code Signing Certificates

For Code Signing Certificates, in addition to the representations and warranties specified in Section 9.6.1.1, GlobalSign represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid:

- **Compliance:** GlobalSign and any Signing Service has complied with the Baseline Requirements for Code Signing and the applicable Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate and operating its PKI or Signing Service;
- **Legal Existence:** For EV Code Signing Certificates, GlobalSign has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Code Signing Certificate was issued, the Subject of the EV Code Signing Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- **Identity of Subscriber**: At the time of issuance, GlobalSign or Signing Service represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 3.2 of this document, (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in GlobalSign's Certificate Policy or Certification Practice Statement;
- **Key Protection:** GlobalSign represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates, or in the case of a Signing Service, securely stored and prevented the misuse of Private Keys associated with Code Signing Certificates; and
- **Subscriber Agreement:** GlobalSign and Signing Service represent that GlobalSign or Signing Service entered into a legally valid and enforceable Subscriber Agreement with the Applicant that satisfies these Requirements or, if they are Affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use.

9.6.1.3. Representations and warranties for EV SSL and EV Code Signing Certificates

For EV SSL and EV Code Signing Certificates, in addition to the representations and warranties specified in Section 9.6.1.1, GlobalSign represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid:

- **Legal Existence:** GlobalSign has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- **Identity:** GlobalSign has confirmed that, as of the date the Certificate was issued, the legal name of the Subject named in the Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- **Right to Use Domain Name:** For EV SSL Certificates, GlobalSign has taken all steps reasonably necessary to verify that, as of the date the Certificate was issued, the Subject named in the Certificate has the right to use all the Domain Name(s) listed in the Certificate;
- **Authorization for EV Certificate:** GlobalSign has taken all steps reasonably necessary to verify that the Subject named in the Certificate has authorized the issuance of the Certificate; and
- **Subscriber Agreement:** The Subject named in the Certificate has entered into a legally valid and enforceable Subscriber Agreement with GlobalSign that satisfies the requirements of these Guidelines or, if they are Affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use.

9.6.1.4. Representations and warranties for NAESB Certificates

For NAESB Certificates, in addition to the representations and warranties specified in Section 9.6.1.1, GlobalSign represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid:

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

9.6.2. RA Representations and Warranties

RAs warrant that:

- Issuance processes are in compliance with this document and the relevant CP;

- All information provided to GlobalSign does not contain any misleading or false information; and
- All translated material provided by the RA is accurate.

9.6.3. Subscriber Representations and Warranties

GlobalSign requires, 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 GlobalSign and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, GlobalSign obtains, for the express benefit of GlobalSign and the Certificate Beneficiaries, either the Applicant's:

1. Agreement to the Subscriber Agreement with GlobalSign; or
2. Acknowledgement of the Terms of Use.

GlobalSign implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant.

For Qualified Certificates, if the Subscriber Agreement is in electronic form, it should be signed with an Advanced Electronic Signature or an Advanced Electronic Seal as specified by Regulation (EU) No 910/2014.

In either case, the Agreement applies to the Certificate to be issued pursuant to the Certificate request.

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 GlobalSign issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use contains 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 following obligations and warranties:

Subscribers and/or Applicants warrant that:

- **Accuracy of Information:** Subscriber will provide accurate and complete information at all times to GlobalSign, both in the Certificate request and as otherwise requested by GlobalSign in connection with issuance of a Certificate;
- **Protection of Private Key:** Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g., password or token; For Code Signing Certificates, Subscriber shall maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 6.2.7.4 of the Baseline Requirements for Code Signing, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). Subscriber represents that it will generate and operate any device storing Private Keys in a secure manner. Subscriber shall use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys. This does not apply to Mark Certificates;
- **Private Key Reuse:** For Code Signing Certificates, Subscriber shall not apply for a Code Signing Certificate if

the Public Key in the Certificate is or will be used with a non-Code Signing Certificate;

- **Acceptance of Certificate:** Subscriber shall not to use the Certificate until after the Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy;
- **Use of Certificate:** For TLS and Mark Certificates, Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use. For S/MIME Certificates, Subscriber shall use the Certificate only on Mailbox Addresses listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use. For Code Signing Certificates, Subscriber shall use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- **Prevention of Misuse:** For Code Signing Certificates, Subscriber shall provide adequate network and other security controls to protect against misuse of the Private Key and that GlobalSign will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys;
- **Reporting and Revocation:** Subscriber accepts the obligation and warranty to promptly cease using a Certificate and its associated Private Key and promptly request that GlobalSign revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code;
- **Sharing of Information**: For Code Signing Certificates, Subscriber acknowledges and accepts that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of Private Key Compromise, discovery of malware, etc.), then GlobalSign is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum;
- **Termination of Use of Certificate:** Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate; and
- **Responsiveness:** Subscriber shall respond to GlobalSign's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours; and
- **Acknowledgment and Acceptance:** Applicant acknowledges and accepts that GlobalSign is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware, or if revocation is required by GlobalSign's CP and/or CPS, or by the applicable Industry Standards.

9.6.3.1. North American Energy Standards Board (NAESB) Subscribers

End entities participating in the Business Practice Standard WEQ-012 v3.0 using Certificates for WEQ-012 applications 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 Standards through GlobalSign as follows:

Each end entity organization shall certify to their certification entity that they have reviewed and acknowledge the following NAESB WEQ PKI Standards.

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

End entity 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.

A. End entity has evaluated each of its selected Certification Authority's Certification Practice Statement in light of those Industry Standards as identified by the Certification Authority;

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

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

- Protect their Private Keys from access by other parties;
- When applicable, identify, through the NAESB EIR, the specific entity they have selected GlobalSign to use as their Authorized Certification Authority;
- Execute all agreements and contracts with GlobalSign as required by GlobalSign's Certification Practice Statement 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 document, e.g., Certificate application procedures, Applicant identity proofing/verification, and Certificate management practices;
- Confirm that it has a PKI Certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to:
    - Certificate Private Key security and handling policy(ies)
    - Certificate revocation policy(ies)

- Identify the type of Subscriber (I.e., individual, role, device, or application) and provide complete and accurate information for each Certificate request;

9.6.4. Relying Party Representations and Warranties

Prior to relying on a Certificate, Relying Parties must accept the Relying Party Agreement and act in accordance with the Relying Party Agreement and this document.

A party relying on a Certificate warrants to:

- Have the technical capability to use Certificates;
- Receive notice of the Issuing CA and associated conditions for Relying Parties;
- Validate an Issuing CA's Certificate by using Certificate status information (e.g., a CRL or OCSP) published by the Issuing CA in accordance with the proper Certificate path validation procedure;
- Trust an Issuing CA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;
- Rely on an Issuing CA's Certificate, only as it may be reasonable under the circumstances; and
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised.

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this document; and
- Take any other precautions prescribed in the Issuing CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

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

9.6.4.1. North American Energy Standards Board (NAESB) Relying Parties

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

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

9.6.4.2. Relying Parties for Qualified Certificates

For Qualified Certificates under the Payment Services Directive (EU) 2015/2366 or Open Banking, a Relying Party must take into account the legislation applicable to Relying Party and the Certificate Subject. At least the following information included in the Certificate must be considered by a Relying Party:

- Competent Authority
- Payment service provider or financial institution

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

EXCEPT TO THE EXTENT PROHIBITED BY LAW OR AS OTHERWISE PROVIDED HEREIN, GLOBALSIGN DISCLAIMS ALL WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

9.8. Limitations of Liability

TO THE EXTENT GLOBALSIGN HAS ISSUED AND MANAGED THE CERTIFICATE IN ACCORDANCE WITH THE CA/BROWSER FORUM REQUIREMENTS, MC REQUIREMENTS AND THIS DOCUMENT, GLOBALSIGN SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE, GLOBALSIGN'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS ($1,000) PER CERTIFICATE; PROVIDED HOWEVER THAT THE LIMITATION SHALL BE TWO THOUSAND DOLLARS ($2,000) PER SUBSCRIBER OR RELYING PARTY PER CERTIFICATE FOR AN EV CERTIFICATE, AN EV CODE SIGNING CERTIFICATE OR MARK CERTIFICATE.

THIS LIABILITY CAP LIMITS DAMAGES RECOVERABLE OUTSIDE OF THE CONTEXT OF THE GLOBALSIGN WARRANTY POLICY. AMOUNTS PAID UNDER THE WARRANTY POLICY ARE SUBJECT TO THEIR OWN LIABILITY CAPS.

IN NO EVENT SHALL GLOBALSIGN BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, RELIANCE UPON, LICENSE, PERFORMANCE OR NON-PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS DOCUMENT.

THE FOREGOING SHALL NOT LIMIT GLOBALSIGN'S LIABILITY WITH RESPECT TO QUALIFIED CERTIFICATES IN ACCORDANCE WITH ARTICLE 13 OF THE EIDAS REGULATION.

9.9. Indemnities

9.9.1. Indemnification by GlobalSign

GlobalSign shall defend, indemnify and hold harmless each Application Software Supplier against any claim, damage, or loss suffered by the Application Software Supplier related to an Extended Validation SSL Certificate or Extended Validation Code Signing Certificate issued by GlobalSign, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Supplier was directly caused by the Application Software Supplier's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) a Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the Application Software Supplier's software failed to check or ignored the status.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify GlobalSign, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this document, or applicable law; (iii) the Compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify GlobalSign, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this document, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. Term and Termination

9.10.1. Term

This document 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

GlobalSign will communicate the conditions and effect of this document termination via the appropriate Repository.

9.11. Individual Notices and Communications with Participants

GlobalSign accepts notices related to this document 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 shall deem 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 to the sender. Individual communications made to GlobalSign must be addressed to: legal@globalsign.com or by post to GlobalSign in the address provided in Section 1.5.2.

9.12. Amendments

9.12.1. Procedure for Amendment

This document is reviewed at least every 365 days and may be reviewed more frequently. All changes are reviewed and approved by the GlobalSign CA Governance Policy Authority.

Changes to this document are indicated by appropriate version numbering.

9.12.2. Notification Mechanism and Period

GlobalSign will post appropriate notice on its web sites of any major or significant changes to this document as well as any appropriate period by when the revised CPS is deemed to be accepted.

9.12.3. Circumstances Under Which OID Must be Changed

No stipulation.

9.13. Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) complaining parties agree to notify GlobalSign of the dispute 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 of 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 this document, parties submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code.

There will be three (3) arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Leuven, Belgium and the arbitrators determine all associated costs.

9.14. Governing Law

This document is governed, construed, and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this document, regardless of the place of residence or place of use of GlobalSign Certificates or other products and services. The law of Belgium applies also to all GlobalSign commercial or contractual relationships in which this document 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

GlobalSign will contractually obligate every RA involved with Certificate issuance to comply with this document 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 document cannot assign their rights or obligations without the prior written consent of GlobalSign.

9.16.3. Severability

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

Each provision of this document 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.

In the event of a conflict between the CA/Browser Forum or MC Requirements and a law, regulation or government order (hereinafter “Law”) of any jurisdiction in which GlobalSign operates or issues Certificates, GlobalSign will modify the conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or Certificate issuances that are subject to that Law.

For TLS, S/MIME and Mark Certificates:

In such event, GlobalSign will immediately (and prior to issuing a Certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification under this section, and the specific modification to the applicable CA/Browser Forum Requirements or MC Requirements implemented.

GlobalSign shall also (prior to issuing a Certificate under the modified requirement) notify the CA/Browser Forum for TLS and S/MIME Certificates, or AuthIndicators Working Group for Mark Certificates.

Any modification to CA practices enabled under this section shall be discontinued if and when the Law no longer applies, or applicable CA/Browser Forum or MC Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this document and a notice to the applicable body or, as outlined above, shall be made within 90 days.

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 document does not waive GlobalSign’s right to enforce the same provisions later or right to enforce any other provisions of this document. 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.

10. Appendix A

10.1. S/MIME BR Certificates

10.1.1. Enterprise RA Requirements

For S/MIME BR Certificates, if company verifies Certificate requests for Subjects within its own organization, company acts as an Enterprise RA and the following requirements apply:

Compliance

Enterprise RA must comply with the provisions of this document and Baseline Requirements for S/MIME that are applicable to the Enterprise RA.

Information Security

Enterprise RA shall apply information security best practices, using Trustworthy Systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

Qualifications

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

Monitoring

GlobalSign has the right to perform monitoring on at least an annual basis of Enterprise RA's adherence with the obligations of this Agreement and this document.

Retention

Enterprise RA shall retain, for at least two (2) years:

All archived documentation relating to the verification, issuance, and revocation of Certificate requests and Certificates 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.

10.1.1.1. Sponsor validated

For Certificates including Individual (Natural Person) attributes in conjunction with the Organization:

Individual information

Enterprise RA shall provide the subject:commonName value in the Certificate request, which must be either the Subject's Personal Name or Pseudonym.

1. A Personal Name shall be a meaningful representation of the Subject's name as verified in the identifying documentation or Enterprise RA records. 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.
2. A Pseudonym shall be an identifier selected by the Enterprise RA which uniquely identifies the Subject of the Certificate within the Organization included in the subject:organizationName attribute.

Collection and retention

Enterprise RA shall collect, validate, and retain evidence of the following identity attributes for the Individual:

1. Given name(s) and surname(s), which shall be current names;
2. Pseudonym (if used);
3. Title (if used); and
4. Further information as needed to uniquely identify the Applicant.

The attributes shall be collected, validated and evidenced based on records (e.g. Active Directory) maintained by Enterprise RA.

Enterprise RA may reuse existing evidence to validate Individual identity if the evidence has been obtained no more than 825 days prior to issuing the Certificate.