GlobalSign Combined Certificate Policy and Certification Practice Statement

eIDAS Certificates for Signing and Timestamping

March 31, 2026

Version 1.0

Table of Contents

Document History

Version	Release Date	Description
1.0	March 31, 2026	Initial release.

Acknowledgments

1. Introduction

1.1. Overview

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

It covers the issuance and lifecycle management of eIDAS Certificates for Signing and Timestamping including certificate status validation services.

NOTE	This document supersedes the GlobalSign Certification Practice Statement (v10.9) and GlobalSign Certificate Policy (v7.9).

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

This document aims to comply with the requirements of:

- eIDAS Regulation
- ETSI 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Certificates; Part 1: General requirements
- ETSI 319 411-2: 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 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - Network Security

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

- CA/Browser Forum Network and Certificate System Security Requirements

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

This document is final and binding between GlobalSign and the Subscriber and/or Relying Party, who uses, relies upon, or attempts to rely upon certification services made available by the Certification Authority referring to this 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 CP/CPS is itself binding upon those Relying Parties.

A Subscriber or Relying Party of a GlobalSign 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.

1.1.1. Certificate Types

The Certificate types covered by this document are the following:

Certificate Type	Description	Applicable requirements	Also sold as
Qualified Certificate for Electronic Signature	Certificates intended to sign documents and forms and to identify an individual, optionally affiliated with a Legal Entity.	ETSI 319 401, ETSI 319 411-1, ETSI 319 411-2, eIDAS Regulation	
Qualified Certificate for Electronic Seal	Certificates intended to sign documents and forms and to identify a Legal Entity.	ETSI 319 401, ETSI 319 411-1, ETSI 319 411-2, ETSI 119 495 (PSD2), eIDAS Regulation	Qualified Trust Seals
Qualified Timestamping	Certificates intended for timestamping.	ETSI 319 401, eIDAS Regulation	

1.2. Document Name and Identification

The name of this document is "Combined Certificate Policy and Certification Practice Statement: eIDAS Certificates for Signing and Timestamping".

This document follows the structure of rfc3647. The OID for GlobalSign NV/SA (GlobalSign) is iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign (4146).

See Appendix C - Certificate Policies for Policy Identifiers governed by this document.

1.3. PKI Participants

1.3.1. Certification Authorities

GlobalSign is a Certification Authority that issues Certificates and performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation.

This document covers the following Root CAs and Issuing CAs with "Qualified" or "Itsme Sign" in the Common Name:

- GlobalSign Document Signing Root R45 with fingerprint

38BE6C7EEB4547D82B9287F243AF32A9DEEB5DC5C9A87A0056F938D91B456A5A

- GlobalSign Document Signing Root E45 with fingerprint F86973BDD0514735E10C1190D0345BF89C77E1C4ADBD3F65963B803FD3C9E1FF
- GlobalSign Timestamping Root R45 with fingerprint 2BCBBFD66282C680491C8CD7735FDBBAB7A8079B127BEC60C535976834399AF7
- GlobalSign Timestamping Root E46 with fingerprint 4774674B94B78F5CCBEF89FDDEBDABBD894A71B55576B8CC5E6876BA3EAB4538

1.3.2. Registration Authorities

GlobalSign acts as the Registration Authority (RA) for Certificates it issues.

GlobalSign may delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process fulfills all of the requirements of Section 3.2.

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 that are applicable to the delegated function; and
4. Comply with (a) this document or (b) the Delegated Third Party's practice statement that GlobalSign has verified complies with the Industry Standards and other applicable requirements.

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 this case, the following Subscriber attributes are validated, pre-defined and constrained by system configuration:

- Organization

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

See Appendix D - Certificate types for product-specific details.

1.3.2.2. Itsme Sign

For Certificates issued by GlobalSign from Itsme Sign CAs:

- Belgian Mobile ID performs the registration services and Subject device provisioning;

- Revocation services are a shared responsibility between GlobalSign and Belgian Mobile ID, for which Belgian Mobile ID serves as the primary contact; and
- A specific Subscriber Agreement for Itsme users is published on the repository.

1.3.3. Subscribers

See definition of “Subscriber” in Appendix B - Definitions and Acronyms.

1.3.4. Relying Parties

See definition of “Relying Party” in Appendix B - Definitions and Acronyms.

1.3.5. Other Participants

No stipulation.

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.

1.4.1. Appropriate Certificate Usage

Subscriber Certificate’s use is restricted by key usage and extended key usage values.

1.4.2. Prohibited Certificate usage

Any usage of a Certificate inconsistent with the key usage and extended key usage extensions included in the Certificate is not authorized. Certificates are not authorized for use for any transactions above the limits that have been indicated in this document.

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.

Certificates issued under this document may not be used:

- For any application requiring fail safe performance
- For any application or mechanism where issues with the Certificate could cause a safety risk (e.g., human or environmental risk)
- Any transaction or data transfer that may result in imprisonment if compromised or falsified.
- Qualified Certificates for Electronic Signatures should only be used by Natural Persons whereas Certificates for Electronic Seals should only be used by legal persons

1.5. Policy Administration

1.5.1. Organization Administering the Document

Requests for information about the compliance of GlobalSign CAs as well as any other inquiry associated with this CPS 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 Certificate Problem Reports for the procedure for Certificate Problem Reports.

1.5.3. Person Determining CP/CPS Suitability for the Policy

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

1.5.4. CP/CPS Approval Procedures

PACOM1 - CA Governance reviews and approves any changes to this document. Upon approval the new version

is published on the GlobalSign Repository at https://www.globalsign.com/repository.

1.6. Definitions and Acronyms

See Appendix B - Definitions and Acronyms

2. Publication and Repository Responsibilities

2.1. Repositories

Revocation information for Subordinate Certificates and Subscriber Certificates is provided as per section Certificate Revocation and Suspension.

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.

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

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

For Certificate revocation requests, GlobalSign authenticates the requests.

3.1. Naming

3.1.1. Types of Names

Certificates are issued with subject DNs (Distinguished Names) in accordance with the Certificate Profiles available in Appendix D - Certificate types. DNs respect name space uniqueness.

3.1.2. Need for Names to be Meaningful

No stipulation.

3.1.3. Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4. Rules for Interpreting Various Name Forms

No stipulation.

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

The validation methods described in the following sections may vary depending on the Subscriber, jurisdiction and Certificate type.

See Appendix D - Certificate types for product-specific details.

3.2.1. Method to Prove Possession of Private Key

No stipulation.

3.2.2. Authentication of Organization and Domain Identity

3.2.2.1. Overview

Organizational identity and address information is verified using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by GlobalSign or a third party who is acting as an agent for GlobalSign; or
4. An Attestation Letter.

GlobalSign verifies the Applicant's right to use the DBA/tradename using the options described above for the verification of the organizational identity and address, or by communication with a government agency responsible for the management of such DBAs or trade names.

Certificates issued to GlobalSign are processed following these processes.

The list of Incorporating Agencies or Registration Agencies (i.e. sources used to verify a Organization's creation, existence, or recognition) is published on the GlobalSign Repository at https://www.globalsign.com/repository under the section "Validation Resources". Additional information on which sources GlobalSign uses during the validation and how GlobalSign validates the suitability of the sources is available in Appendix D - Certificate types.

3.2.3. Authentication of Individual identity

Information related to the Individual includes the Individual's (full legal) name and further information as needed to uniquely identify the Individual. This may include but is not limited to residential address, date of birth, place of birth, government issued document number, or unique identifier of eID means.

Individual identity information and address information included in a Certificate Request is verified using a physical or digital identity document, using an eID scheme, a Digital Signature based on a Certificate that provides a sufficient level of security and validation for the Certificate requested, or a verified letter of attestation.

GlobalSign accepts a government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

- passport;
- driver's license;
- personal identification card;
- concealed weapons permit; or

- military ID.

GlobalSign may rely on additional sources to verify further information as needed to uniquely identify an Individual: official documents (including government issued tax documents, court orders, marriage certificates), government or regulatory registers, national population registers, utility bill, bank statement, credit card statement, or other form of identification that GlobalSign determines to be reliable.

See Appendix D - Certificate types for product-specific details.

3.2.4. Non-verified Subscriber Information

No stipulation.

3.2.5. Validation of Authority

GlobalSign verifies the authenticity of the received Certificate request with either the Applicant or the Applicant's representative(s) using the following methods:

1. a reliable or verified method of communication belonging to the Applicant (or a Parent/Subsidiary or Affiliate) to contact the Applicant or the Applicant's representative(s)
2. verified letters of attestation; or
3. approval via the GlobalSign account; or
4. use of a signing process that identifies the signer; or
5. a Digital Signature based on a Certificate that provides a sufficient level of security and validation for the Certificate requested. GlobalSign verifies that the signing Certificate was issued by a CA qualified by the entity responsible for adopting, enforcing, or maintaining the adopted standard and chains to an intermediate Certificate or Root Certificate designated as complying with such standard.

GlobalSign verifies the authenticity of the request directly with the representative named during the application process. Alternatively, GlobalSign can confirm the authenticity of the request with an authoritative source within the Subscriber's organization, such as the Subscriber's main business offices, corporate offices, human resource offices, information technology offices, or any other person or department that GlobalSign deems appropriate.

Not all validation methods will be acceptable in all circumstances or be available to use for all types of information. See Appendix D - Certificate types for product-specific details.

3.2.6. Criteria for Interoperation

Cross Certificates are published in the GlobalSign Repository.

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 performed using the same method as during initial Certificate issuance or a method with similar assurance.

Identification of the request is subject to the 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 Certificate Revocation and Suspension.

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 will consider an application from a non-sanctioned Individual or Organization from a non-sanctioned country or a country where GlobalSign is prohibited from doing business.

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.

Applicants must submit sufficient information to perform the required verification.

The enrollment process consists of the following steps:

- Applicant provides the Public Key to be included in the Certificate (e.g. CSR);
- Applicant provides the details to be included in the Certificate;
- Acceptance of the Subscriber Agreement and/or other applicable terms and conditions; and
- Applicant provides any other details requested by GlobalSign.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

GlobalSign performs all identification and authentication functions in accordance with Section 3.2.

GlobalSign relies on documents and data provided in Section 3.2 to verify Certificate information, or may reuse previous validations. See Appendix D - Certificate types for product-specific information on age of validated data and conditions of re-use.

In no case is a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

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.

When external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

For keys generated by Subjects, GlobalSign ensures that the Certificate request process provides reasonable assurance that the Subject has possession or control of the Private Key associated with the Public Key presented for certification

4.2.2. Approval or Rejection of Certificate Applications

Approval requires successful completion of validation per Section 3.2.

GlobalSign maintains criteria and internal databases, including individuals entities for 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 for screening Applicants.

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

4.2.3. Time to Process Certificate Applications

GlobalSign ensures that all reasonable methods are used to evaluate and process Certificate applications. Certificate requests are typically processed within 24-96 hours.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

For issuance from Root CAs, an authorized individual is required to issue a direct command to perform a Certificate signing operation.

For issuance of Subscriber Certificates, when the required authentication and identification processes have been completed, the Certificate is linted and, upon successful linting, signed by the Issuing CA and provided to the Subscriber.

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

GlobalSign notifies the Subscriber or its representative of the issuance of a Certificate via one of the contact methods supplied by the Subscriber during the enrollment process or by any other equivalent method.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Subscriber must review and verify Certificate contents before using the Certificate.

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

4.4.2. Publication of the Certificate by the CA

Root CA Certificates and Qualified Timestamping Certificates are available on the public repository.

Subscriber Certificates are provided to Subscribers during Certificate delivery.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscriber Private Keys and Certificates must be used in accordance with the Subscriber Agreement.

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.

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

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

As per Conduct Constituting Certificate Acceptance.

4.6.6. Publication of the Renewal Certificate by the CA

As per Publication of the Certificate by the CA.

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 to replace a compromised Private Key prior to revocation.

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 Notifications to Subscriber by the CA of Issuance of Certificate.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

As per Conduct Constituting Certificate Acceptance.

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

As per Publication of the Certificate by the CA.

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 Public Key.

Certificate modification requests are processed as new Certificate requests when the validity period is changed or the 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.

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 Notifications to Subscriber by the CA of Issuance of Certificate.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

As per Conduct Constituting Certificate Acceptance.

4.8.6. Publication of the Modified Certificate by the CA

As per Publication of the Certificate by the CA.

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 and Timelines 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 that GlobalSign revokes the Certificate;
2. The Subscriber notifies GlobalSign that the original Certificate request was not authorized and does not retroactively grant authorization;
3. GlobalSign obtains 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); or
5. GlobalSign receives notice or otherwise becomes aware of unexpected termination of a Subscriber's or

Subject's agreement or business functions.

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 of Section 6.1.5 and Section 6.1.6;
2. GlobalSign obtains evidence that the Certificate was misused;
3. GlobalSign is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. GlobalSign is made aware of a material change in the information contained in the Certificate;
5. GlobalSign is made aware that the Certificate was not issued in accordance with the applicable Industry Standards or this CP/CPS;
6. GlobalSign determines or is made aware that any of the information appearing in the Certificate is inaccurate;
7. 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;
8. Revocation is required by this CP/CPS; or
9. 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.

Nothing herein prohibits GlobalSign from revoking a Certificate prior to these time frames.

See Appendix D - Certificate types for additional product-specific circumstances and timelines for revocation.

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; or

10. Death of a Subscriber.

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

1. The Subordinate CA requests 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/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; or
9. Revocation is required by this document.

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

- 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 and no revocation reason will be included in the CRL.

Belgian Mobile ID is the initial point of contact for revocation requests for Certificates issued from Itsme Sign CAs.

4.9.2. Who Can Request Revocation

GlobalSign, Subscriber or RA can initiate revocation.

Alternatively, GlobalSign allows Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties to submit Certificate Problem Reports to notify GlobalSign of a suspected reasonable cause to revoke the Certificate.

4.9.3. Procedure for Revocation Request

4.9.3.1. Certificate Revocation Requests

For revocation requests from Subscribers, GlobalSign may provide automated mechanisms to request revocation within the Subscriber's portal.

Requests for revocation can also be sent to report-abuse@globalsign.com.

Out of band methods may be used to authenticate these revocation requests, such as receipt of a fax/letter/phone call, the origins of which must be authenticated using shared secrets from the account. Alternatively, methods may be used which rely on a demonstration of control of one or more elements of the Subject DN of the Certificate. In these cases, the timeline for revocation as stated in Section 4.9.1. starts from the moment the revocation request has been authenticated.

GlobalSign will record each request for revocation and authenticate the source, and if the revocation request cannot be confirmed, records the actions taken along with the justification.

Certificate Problem Reports

Certificate Problem Reports are reports informing GlobalSign of reasonable cause to revoke the Certificate. 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.

To verify the claims made in Certificate Problem Reports, they 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). Without this proof, GlobalSign cannot consider the key as compromised.

- 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.

Short-term Certificates

For short-term Certificates issued through the GlobalSign Digital Signing Service products, revocation is not supported.

Notifications for problems with these non-revocable Certificates or requests for information on these potential notified problems must be sent to report-abuse@globalsign.com.

GlobalSign records any reported issue with such a Certificate.

For the identity of the reported Certificate, a notification or request for information 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).

4.9.4. Revocation Request Grace Period

The revocation request grace period is the time available for a Subscriber to take any necessary actions themselves to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate.

Subscribers must inform GlobalSign within 48 hours 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.

See Appendix D - Certificate types for product-specific requirements.

4.9.6. Revocation Checking Requirements for Relying Parties

Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and that the Certificate is valid by consulting the CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete, otherwise all warranties become void.

Respective CRL and OCSP location information are provided within Certificates.

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.

For Qualified Certificates, validation of the Certificate chain must be carried out successfully up to the GlobalSign trust anchor within the relevant EU trusted list.

4.9.7. CRL Issuance Frequency

For CAs issuing Subscriber Certificates with CRLs:

- GlobalSign updates and publishes a new CRL at least every twenty-four (24) hours; and
- The value of the nextUpdate field will not be more than ten days beyond the value of the thisUpdate field.

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 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 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

See Section Circumstances and Timelines for Revocation.

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.

GlobalSign accepts 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 this document accordingly if the new method of submission is accepted.

4.9.13. Circumstances for Suspension

No stipulation.

4.9.14. Who Can Request Suspension

No stipulation.

4.9.15. Procedure for Suspension Request

No stipulation.

4.9.16. Limits on Suspension Period

No stipulation.

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, depending on the Issuing CA. The integrity and authenticity of this status information is secured and protected.

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

For Issuing CAs providing only CRL, GlobalSign does not remove from the CRL revoked Certificates after they have expired. If OCSP is provided, revocation entries may be removed after expiry of the Certificate to promote more efficient CRL file size management.

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 check the status of 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

No stipulation.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

GlobalSign does not offer key escrow services to Subscribers.

CA Private Keys are not escrowed.

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 GlobalSign 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 GlobalSign 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, 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

GlobalSign maintains off-site backup copies with equivalent security controls as the primary backups.

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

Individual 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.

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 and documented in the job description.

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 GlobalSign on the Information verification requirements outlined in the applicable Industry Standards.

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 seven (7) 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).

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 GlobalSign 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 seven (7) 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 seven (7) 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.

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. Recovery Procedures after Key Compromise

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;
- 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; and
- 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, Relying Parties, Application Software Providers, and other relevant stakeholders;
- 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 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.

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; and
- 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

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

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 4.9.1.1; 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).

Refer to the sections Key protection and verification in Appendix D - Certificate types.

For Qualified Certificate types where specific Subscriber Private Key protection requirements apply, GlobalSign will contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection.

6.1.2. Private Key Delivery to Subscriber

Parties other than the Subscriber shall not archive the Subscriber Private Key without authorization by the Subscriber.

If GlobalSign or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, GlobalSign will revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3. Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4. CA Public Key Delivery to Relying Parties

GlobalSign Public Keys are provided to Relying Parties as part of browser, operating system or trusted lists of root programs.

Relying Parties may also obtain GlobalSign Public Keys from GlobalSign's repository or website.

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 3072 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.

6.1.6. 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)

No stipulation.

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

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates;
3. Certificates for infrastructure purposes (administrative role Certificates, internal CA operational device Certificates);
4. Certificates for OCSP Response verification; and
5. Signatures for OCSP Responses.

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.

6.2.1.3. Subscriber Private Key Standards and Controls

See Appendix D - Certificate types for product-specific requirement.

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 CA Private Keys.

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.

For Subscriber Keys, refer to Section Subscriber Key Pair Generation for Private Key Storage practices.

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.

6.2.10. 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 Cryptographic Module Standards and Controls.

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

Certificates have a maximum validity period of:

6.3.2.1. Root and Issuing CAs

Certificate Type	Maximum Validity Period
Root CA	25 years
Subordinate CA	18 years

6.3.2.2. Subscriber Certificates

Certificate Type	Maximum Validity Period

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

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.

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; and
- 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.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

Certificates are issued in accordance with the profile requirements of ETSI 319 412 part 1 to 5.

7.1.1. Version Number(s)

GlobalSign issues Certificates of type X.509 Version 3.

7.1.2. Certificate Extensions

GlobalSign issues Certificates which conform to RFC 5280. Qualified Certificates for Electronic Signatures and Seals include the QCStatements extension.

7.1.3. Algorithm Object Identifiers

7.1.3.1. SubjectPublicKeyInfo

GlobalSign indicates an RSA key within the subjectPublicKeyInfo field within a Certificate or precertificate using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters will be present and shall be an explicit NULL.

GlobalSign indicates an ECDSA key within the subjectPublicKeyInfo field within a Certificate or precertificate using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters use the namedCurve encoding:

- For P-256 keys, the namedCurve shall be secp256r1 (OID: 1.2.840.10045.3.1.7), or
- For P-384 keys, the namedCurve shall be secp384r1 (OID: 1.3.132.0.34)
- For P-521 keys, the namedCurve shall be secp521r1 (OID: 1.3.132.0.35)

7.1.3.2. Signature AlgorithmIdentifier

All objects signed by a CA Private Key conforming to this document on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, the following algorithms apply to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList

- The signatureAlgorithm field of a BasicOCSPResponse.

Only the following algorithms shall be used.

RSA signature
RSASSA-PKCS1-v1_5 with SHA-256
RSASSA-PKCS1-v1_5 with SHA-384
RSASSA-PKCS1-v1_5 with SHA-512
RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes
RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes
RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes

ECDSA signature	Signature Algorithm
signing key P-256	signature shall use ECDSA with SHA-256
signing key P-384	signature shall use ECDSA with SHA-384
signing key P-521	signature shall use ECDSA with SHA-512

7.1.4. Name Forms

GlobalSign issues Certificates with name forms compliant to RFC 5280

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

See Appendix C - Certificate Policies.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

GlobalSign issues Certificates with policy qualifiers set as per Appendix C - Certificate Policies.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

GlobalSign issues “full and complete” CRLs and does not issue “partitioned” CRLs.

7.2.1. Version Number(s)

GlobalSign issues X.509v2 CRLs in compliance with RFC 5280.

7.2.2. CRL and CRL Entry Extensions

The reasonCode extension is present for CRL entries for Root CA’s, Subordinate CA’s, Cross Certificates and may be present for other Certificate types.

If present, the reasonCode (OID 2.5.29.21) extension SHALL NOT be marked critical.

The CRLreason of certificateHold (6) SHALL NOT be used for Root CA or Subordinate CA Certificates.

If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted, subject to the following requirements.

If a reasonCode CRL entry extension is present, the CRLReason SHALL indicate the most appropriate reason for revocation of the Certificate.

7.3. OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross-Certified Subordinate CA Certificates, and that Certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1. Version Number(s)

GlobalSign issues Version 1 OCSP responses.

7.3.2. OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

At all times, GlobalSign:

1. Complies with the applicable requirements for the Certificate type;
2. Complies with the audit requirements set forth in this section; and
3. Is licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1. Frequency and Circumstances of Assessment

Compliance audits are performed on an annual basis.

8.2. Identity/Qualifications of Assessor

Audits are performed by a Qualified Auditor. A Qualified Auditor means a Natural Person, Legal Entity, or group of Natural Persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section Topics Covered by Assessment);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

For eIDAS, the audit 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 against the requirements of the eIDAS Regulation (EU) No 910/2014.

8.3. Assessor’s Relationship to Assessed Entity

GlobalSign selects an assessor who is independent from GlobalSign.

8.4. Topics Covered by Assessment

eIDAS audits cover:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- 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 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 EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (“ETSI 319 421”)
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking (“ETSI 119 495”)

WebTrust audits cover:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - Network Security

8.5. Actions Taken as a Result of Deficiency

If presented with a material non-compliance by auditors, GlobalSign creates a corrective action plan to resolve the deficiency.

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.

8.7. Self-Audit

GlobalSign monitors its adherence to this document and the requirements specified in the Overview section 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 of the Certificates issued.

8.8. Review of delegated parties

Except for Delegated Third Parties, Enterprise RAs, and Technically Constrained Subordinate CAs that undergo an annual audit that meets the criteria specified in Section 8.4, GlobalSign ensures the practices and procedures of delegated parties are in compliance with the applicable Industry Standards and this document. GlobalSign documents the obligations of delegated parties and perform 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

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End Entities

No stipulation.

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, GlobalSign has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

For additional product-specific CA representations and warranties, See Appendix D - Certificate types.

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;
- **Acceptance of Certificate:** Subscriber shall not use the Certificate until after the Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy.
- **Reporting and Revocation:** Subscriber accepts the obligation and warranty to (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate; or (c) there is evidence that the Certificate was used to sign Suspect Code;
- **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
- **Responsiveness:** Subscriber shall respond to GlobalSign's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours
- **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 revocation is required by this document, or by the applicable Industry Standards.

For additional product-specific Subscriber representations and warranties, See Appendix D - Certificate types.

9.6.4. Relying Party Representations and Warranties

Prior to relying on a Certificate, Relying Parties must accept the following:

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. 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 INDUSTRY STANDARDS 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 SUBSCRIBER OR RELYING PARTY PER CERTIFICATE.

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

No stipulation.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify GlobalSign, its partners, and any Trusted Root entities, 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. Individuals' communications made to GlobalSign must be addressed to: legal@globalsign.com or by post to GlobalSign at 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 version is deemed to be accepted. Any updates become binding for all Certificates that have been issued or are to be issued upon the effective date of the updated version of this document.

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 CP/CPS, 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.

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 B - Definitions and Acronyms

10.1. Definitions

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

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.

Belgian Mobile ID: Belgian Mobile ID NV/SA, a Legal Entity registered in Belgium with company number 0541.659.084.

CA/Browser Forum Requirements: means the current versions of the CA/Browser Forum Requirements in Section Overview.

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

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom GlobalSign 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 Authority: See Certificate Authority.

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

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.

Digital Signing Service: A remote signing service based on AATL Certificates, where the key is managed on behalf of the Subscriber.

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 platform that enables an Enterprise RA to issue various client Certificates using pre-validated identities and domains.

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.

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.).

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.

Individual: A Natural Person.

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.

Industry Standards: The applicable requirements defined in Section Certificate Types.

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.

Natural Person: An Individual; a human being as distinguished from a Legal Entity.

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

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

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

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

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

Qualified Certificate for Electronic Seals: A Certificate for Electronic Seals, that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex III of the eIDAS Regulation.

Qualified Certificate for Electronic Signature: A Certificate for Electronic Signatures, that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex I of the eIDAS Regulation.
Qualified Electronic Seals: An advanced Electronic Seal, which is created by a Qualified Electronic Seal Creation Device, and that is based on a Qualified Certificate for Electronic Seal.

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

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

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

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

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

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.

Requirements: the requirements defined in Section Overview.

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.

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

Root CA: The top-level Certification Authority whose Root Certificate is distributed by Application Software

Suppliers and that issues Subordinate CA Certificates.

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

Subject: The Natural Person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. 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.

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

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate.

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

Validation Specialist: Someone who performs the information verification duties.

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

10.2. Acronyms

API Application Programming Interface

ARL Authority Revocation List (A CRL for Issuing CAs rather than end entities)

CA Certification Authority

ccTLD Country Code Top-Level Domain

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

DBA Doing Business As

DNS Domain Name System

DSS Digital Signing Service

EKU Extended Key Usage

EPKI Enterprise PKI

FIPS (US Government) Federal Information Processing Standard

FQDN Fully Qualified Domain Name

HSM Hardware Security Module

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

MSSL Managed SSL

NAESB North American Energy Standards Board

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

QGIS Qualified Government Information Source

QIIS Qualified Independent Information Source

RA Registration Authority

RFC Request for Comments

S/MIME Secure MIME (Multipurpose Internet Mail Extensions)

SSL Secure Sockets Layer

TLD Top-Level Domain

TLS Transport Layer Security

TLS BR Baseline Requirements (for TLS)

11. Appendix C - Certificate Policies

GlobalSign organizes its OID arcs for the various Certificate Types described in this document as follows:

Category	OID	Description	Private Key
Qualified	**1.3.6.1.4.1.4146.1.40.36**	**eIDAS Qualified Certificates - QSCD**	
	1.3.6.1.4.1.4146.1.40.36.1	Qualified Certificates for Electronic Signatures	Private Key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.36.2	Qualified Certificates for Electronic Seals	Private Key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37	**eIDAS Qualified Certificates – Non QSCD**	
	1.3.6.1.4.1.4146.1.40.37.1	Qualified Certificates for Electronic Signatures	Private Key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37.2	Qualified Certificates for Electronic Seals	Private Key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37.3	Qualified Certificates for Electronic Seals - Open Banking	Private Key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.38	**eIDAS Qualified Certificates – Remote QSCD**	
	1.3.6.1.4.1.4146.1.40.38.1	Qualified Certificates for Electronic Signatures	Private Key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.38.2	Qualified Certificates for Electronic Seals	Private Key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41	**eIDAS Qualified Certificates – Remote Non QSCD**	
	1.3.6.1.4.1.4146.1.40.41.1	Qualified Certificates for Electronic Signatures	Private Key not on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41.2	Qualified Certificates for Electronic Seals	Private Key not on QSCD Managed on behalf of Subscriber
Timestamping	1.3.6.1.4.1.4146.1.32	Timestamping Certificate Policy – Certificates for Qualified Timestamping (QTS) under eIDAS Regulation	

Community OIDs

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

Community	OID	Description
ETSI	0.4.0.194112.1.0	QCP-n: Certificate Policy for EU Qualified Certificates issued to Natural Persons
	0.4.0.194112.1.1	QCP-l: Certificate Policy for EU Qualified Certificates issued to legal persons
	0.4.0.194112.1.2	QCP-n-qscd: Certificate Policy for EU Qualified Certificates issued to natural persons with Private Key related to the certified Public Key in a QSCD
	0.4.0.194112.1.3	QCP-l-qscd: Certificate Policy for EU Qualified Certificates issued to legal persons with Private Key related to the certified Public Key in a QSCD

12. Appendix D - Certificate types

This appendix contains product-specific practices that apply on top of the general provisions in Sections 1–9 and must be read together with the relevant Sections.

12.1. Qualified Certificate for Electronic Seals

12.1.1. Product description

Qualified Certificates for Electronic Seals are intended to digitally sign documents and forms. They identify an organization, and, where applicable, PSD2 attributes.

These Certificates are issued in accordance with the eIDAS Regulation, as well as ETSI EN 319 411-1, ETSI EN 319 411-2 and, where applicable, ETSI TS 119 495.

12.1.2. Identity proofing

GlobalSign checks that Certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

GlobalSign validates the information below in accordance with the totality of

- article 24 of the eIDAS Regulation and
- Section 6.2.2. Initial identity validation of both
  - ETSI EN 319 411-1 and
  - ETSI EN 319 411-2.
  - (optionally) ETSI TS 119 495.

GlobalSign collects and validates either direct evidence or an attestation from an appropriate and authorized source. All relevant registration information and validation documentation is recorded. This information may be accessed in line with GlobalSign's Privacy Policy.

12.1.2.1. Authorized Representative Identity

GlobalSign collects the following information for the individual:

- Given name(s) and surname(s)
- Further information as needed to uniquely identify the Individual. This may include but is not limited to residential address, date of birth, place of birth, government issued document number, unique identifier of eID means.

GlobalSign validates this information either directly or by relying on a third party in accordance with national law.

Additionally, the Applicant provides contact information.

12.1.2.2. Organizational identity

GlobalSign collects and validates the following information:

- Organization Identity, including:
  - Formal name of the Legal Entity and legal status;
  - A registered Assumed Name for 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, 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.
- Affiliation of the Natural Person to the legal person See section; and
- Approval of the Certificate request;

12.1.2.3. PSD2 attributes

GlobalSign validates the following PSD2 attributes in accordance with 6.2.2 Initial identity validation of ETSI TS 119 495:

- the role(s) of the payment service provider
- An Authorization Number, or other identifier recognized by the Competent Authority
- the Competent Authority where the payment service provider is registered.

If applicable, GlobalSign sends an email to the Competent Authority mentioned in a newly issued Certificate using a notified email address.

12.1.3. Age of validated data

GlobalSign may reuse previous validations provided that:

- GlobalSign obtained the data or document 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.

GlobalSign may reuse a previously submitted Subscriber Agreement in support of multiple Qualified Certificates containing the same Subject. GlobalSign sets no limit on how many Certificates are allowed to be issued to the

same Subscriber after the initial identity validation.

After the change to any validation method, GlobalSign may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this section unless otherwise specifically provided in the applicable requirements.

The time period set forth above begins to run on the date the information was collected.

12.1.4. Circumstances and timelines for revocation

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

- 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.

12.1.5. Key protection and verification

For Qualified Certificates issued in accordance with QCP-l profile, a secure cryptographic device is optional.

For Qualified Certificates issued in accordance with QCP-l-qscd profile, the Private Key must be generated and stored in a QSCD.

GlobalSign offers remote signing with Qualified Certificates for Electronic Seals (QCP-l profile) through its Digital Signing Service, in which case Private Keys are generated, stored and managed on behalf of Subscribers 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).

GlobalSign monitors the QSCD certification status, and appropriate measures, including revocation, will be taken if the certification status of a QSCD changes.

Private Keys may be managed by GlobalSign or a third party on behalf of a Subject. If a Private Key is managed on behalf of a Subject, GlobalSign shall ensure that the Subject (i.e. legal person) maintains control over its Private Key. For keys managed by a third party, GlobalSign shall confirm that the third party is a Qualified Trust Service Provider and ensures sole control.

If a Private Key resides on a QSCD and GlobalSign or a third party manages the QSCD for the Subject, the Private Key shall not be used for signing except within a QSCD. The Subject's Key Pair should be used only for Electronic Seals.

GlobalSign only generates Private Keys if GlobalSign manages the Private Key on behalf of the Subscriber.

For any devices managed by a third party TSP (i.e. not GlobalSign) on behalf of the Subject, GlobalSign shall verify that this third party TSP is meeting the appropriate requirements.

12.2. Qualified Certificate for Electronic Signatures

12.2.1. Product description

Qualified Certificates for Electronic Signatures are intended to digitally sign documents and forms.

They identify either:

- an Individual; or
- an Individual affiliated with an organization;

These Certificates are issued in accordance with the eIDAS Regulation, as well as ETSI EN 319 411-1 and ETSI EN 319 411-2.

12.2.2. Identity proofing

GlobalSign checks that Certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

GlobalSign validates the following information in accordance with the totality of

- article 24 of the eIDAS Regulation and
- Section 6.2.2. Initial identity validation of both
  - ETSI EN 319 411-1 and
  - ETSI EN 319 411-2.

GlobalSign collects and validates either direct evidence or an attestation from an appropriate and authorized source. All relevant registration information and validation documentation is recorded. This information may be accessed in line with GlobalSign's Privacy Policy.

12.2.2.1. Individual identity

GlobalSign collects the following information for the individual:

- Given name(s) and surname(s)
- Further information as needed to uniquely identify the Individual. This may include but is not limited to residential address, date of birth, place of birth, government issued document number, unique identifier of eID means.

GlobalSign validates this information either directly or by relying on a third party in accordance with national law.

Additionally, the Applicant provides contact information.

12.2.2.2. Organizational identity

In the case of Individual affiliated with an organization, GlobalSign additionally collects and validates the following information:

- Organization Identity, including:
  - Formal name of the Legal Entity and legal status;
  - A registered Assumed Name for 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, 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.
- Affiliation of the Natural Person to the legal person;
- Approval by the legal person and the Natural Person;

If an Organization subscribes to GlobalSign's services to issue Certificates to itself or its members, GlobalSign validates that:

- Subscriber is authorized to act for the Subject as identified (e.g. is authorized for all members of the identified organization);
- if the Subscriber is an organization, the authorized representative is allowed to represent the organization and is entitled to request Certificates for that organization or its members.

12.2.3. Age of validated data

GlobalSign may reuse previous validations provided that:

- GlobalSign obtained the data or document 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.

GlobalSign may reuse a previously submitted Subscriber Agreement in support of multiple Qualified Certificates containing the same Subject. GlobalSign sets no limit on how many Certificates are allowed to be issued to the same Subscriber after the initial identity validation.

After the change to any validation method, GlobalSign may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this section unless otherwise

specifically provided in the applicable requirements.

The time period set forth above begins to run on the date the information was collected.

12.2.4. Key protection and verification

For Qualified Certificates issued in accordance with QCP-n profile, a secure cryptographic device is optional.

For Qualified Certificates issued in accordance with QCP-n-qscd profile, the Private Key must be generated and stored in a QSCD.

GlobalSign monitors the QSCD certification status, and appropriate measures, including revocation, will be taken if the certification status of a QSCD changes.

Private Keys may be managed by GlobalSign or a third party on behalf of a Subject. If a Private Key is managed on behalf of a Subject, GlobalSign shall ensure that the Subject maintains sole control over its Private Key. For keys managed by a third party, GlobalSign shall confirm that the third party is a Qualified Trust Service Provider and ensures sole control.

If a Private Key resides on a QSCD and GlobalSign or a third party manages the QSCD for the Subject, the Private Key shall not be used for signing except within a QSCD. The Subject's Key Pair should be used only for Electronic Signatures.

GlobalSign only generates Private Keys if GlobalSign manages the Private Key on behalf of the Subscriber.

For any devices managed by a third party TSP (i.e. not GlobalSign) on behalf of the Subject, GlobalSign shall verify that this third party TSP is meeting the appropriate requirements.

12.3. Qualified Timestamping

12.3.1. Product description

Certificates for Qualified Timestamping are intended to digitally sign timestamps.

They:

- establish evidence that signed data existed at a specific date/time by binding the date and time to data based on an accurate time source linked to Coordinated Universal Time; and
- bind the date and time to data in a manner as to reasonably preclude the possibility of the data being changed undetectably;

These Certificates are issued in accordance with the eIDAS Regulation, as well as ETSI EN 319 421.

12.3.2. Identity proofing

Qualified Timestamping Certificates are issued to GlobalSign as the Subscriber, where the organizationName

attribute is set to "GlobalSign nv-sa", countryName attribute is set to "BE", organizationIdentifier is set to "NTRBE-0459134256" and the commonName attribute identifies which timestamp unit was used.