GlobalSign
Certification Practice Statement

Date: March 31, 2020

Effective date for Qualified Timestamping, Qualified Web Authentication Certificates, Qualified Certificates for Electronic Signatures and Qualified Certificates for Electronic Seals: {normal date + 2 weeks}

Version: v9.3

Table of Contents

Document History

Version	Release Date	Author(s)	Status & Description
V5.0	07/10/05	Various Authors	Various changes leading up to a rewrite to support Extended Validation
V5.5	06/19/07		
V5.6	06/25/07	Steve Roylance	Final modification for EV Issue 1.0
V6.0	12/17/07	Steve Roylance	Major Release supporting new Certificate life cycle solutions
V6.1	05/20/08	Steve Roylance	Administrative update/ clarifications
V6.2	10/13/08	Steve Roylance	Administrative update/ clarifications
V6.3	12/16/08	Steve Roylance	Administrative update/ clarifications
V6.4	02/11/09	Steve Roylance	Administrative update/clarifications
V6.5	05/12/09	Steve Roylance	Administrative update/clarifications
V6.6	02/03/10	Lila Kee	Administrative update
V6.7	05/12/10	Johan Sys	Administrative update/clarifications
V7.0	03/22/12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CA/B Forum Baseline Requirements for issuance of SSL Certificates
V7.1	03/29/12	Lila Kee and Steve Roylance	Addition of support for NAESB and incorporation of the AlphaSSL product range
V7.2	06/07/12	Steve Roylance	Additional CA/B Forum Baseline Requirements
V7.3	07/01/12	Steve Roylance	Final CA/B Forum Baseline Requirements
V7.4	03/15/13	Giichi Ishii Lila Kee	Extended validity period of Personal Sign, Administrative updates/clarifications Modification to NAESB Certificates incorporating WEQ-012 v 3.0 updates
V7.5	03/31/13	Giichi Ishii	Statement of compliance to CA/Browser Forum Baseline Requirement, EPKI specification update
V7.6	03/07/14	Giichi Ishii Carolyn Oldenburg	Modified validity period for timestamping Certificate Added Certificate Data in the scope of archive Administrative updates/clarifications
V7.7	04/25/14	Giichi Ishii	Modified availability requirement and maximum process time for revocation Administrative update/clarifications
V7.8	02/09/14	Steve Roylance	Modifications to enhance the description of domain validation processes, highlighted by public review.
V7.9	02/25/15	Carolyn Oldenburg Steve Roylance Giichi Ishii	Modified maximum validity period of Code Signing certificate. GlobalSign's new R6 root and readability enhancements to cover new AATL offerings
V8.0	08/20/15	Doug Beattie Lila Kee Steve Roylance	Support for IntranetSSL, Hosted Root™, alternative OIDs and Publication of all Subordinate CAs which are non-constrained.
V8.1	05/02/16	Lila Kee	Annual Review Modified NAESB EIR requirements to reflect non WEQ energy participants requirements
V8.2	06/16/16	Steve Roylance	Adding R7 and R8 Root certificates
V8.3	08/11/16	Giichi Ishii	Clarification on Certificate Transparency Adding Test CA OID
V8.4	01/17/17	Giichi Ishii Carolyn Oldenburg Lila Kee	CA/B Forum Ballot 173 Removal of Root R2 & R4 Addition of Minimum Requirements for Code Signing Certificates
V8.5	08/07/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie	Updates for AATL Digital Signing Service Added CAA record checking requirement Annual update/review to fix bugs
V8.6	15/12/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie	Updates related to Annual BR assessment

		Simon Labram	
V8.7	03/04/18	Doug Beattie Lila Kee	Max SSL validity set to 825 days Specified that GlobalSign no longer generates keys for SSL certificates Updates for NAESB identify requirements
V8.8	06/15/18	Various authors	Updates for Qualified Certificates Removed Method #5 to comply with BR domain validation practices.
V8.9	10/11/18	Giichi Ishii Arvid Vermote Doug Beattie Carolyn Oldenburg	Updates to revocation timelines in accordance with CABF Ballot SC6 Made a variety of definition/acronym updates for clarification
V9	03/12/19	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Updated roles requiring separation of duties Added new ICAs for AATL and Timestamping Added new Email Domain Validation methods and definitions Added new Phone Domain Validation methods and definitions Added new IoT policy OIDs
V9.1	05/30/2019	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Added new GlobalSign R46/E46 Root Certificates Added new Private Client Certificate Policy OID Support for Qualified Timestamping and Qualified Web Authentication Certificates Changed “re-key” definition to match WebTrust
V9.2	09/25/2019	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Removed references to NAESB High Assurance certificates Removed “any other” method for IP Address approval
V9.3	03/31/2020	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Added non-TLS roots Updated address in section 1.5 Added more detail to AATL Individual/Organization vetting requirements Added new Timestamping Token OID Added advanced electronic signature/seal (or higher) as an alternative means to confirm authority following COVID-19 emergency Added notification period for subscribers regarding expiration of certificates Added new CABF code signing requirements

Acknowledgments

This GlobalSign CPS conforms to:

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

This GlobalSign CPS conforms to current versions of the requirements of the following schemes:

- AICPA/CICA, WebTrust 2.1 Program for Certification Authorities
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria
- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/B Forum Network and Certificate System Security Requirements
- CA/B Forum EV Code Signing Certificate Guidelines
- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- Browsers’ root programs

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

1.0 Introduction

This Certification Practice Statement (CPS) applies to the products and services of GlobalSign nv/sa. Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. GlobalSign nv/sa may also provide additional services, such as timestamping. This CPS may be updated from time to time as outlined in Section 1.5 *Policy Administration*. The latest version may be found on the GlobalSign group company Repository at https://www.globalsign.com/repository. (*Alternative language versions may be available to aid Relying Parties and Subscribers in their understanding of this CPS; however, in the event of any inconsistency, the English language version shall control.)*

A CPS highlights the "procedures under which a Digital Certificate is issued to a particular community and/or class of application with common security requirements." This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format (RFC 3647 obsoletes RFC 2527). An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and Certificate management. While certain section titles are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply to services of GlobalSign nv/sa. These sections state 'No stipulation.' Additional information is presented in subsections of the standard structure where necessary. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides Relying Parties with advance notice of GlobalSign's practices and procedures. GlobalSign nv/sa conforms to the current version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the "Baseline Requirements), the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (the "EV Guidelines"), CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (the "EV Code Signing Guidelines"), and Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (the "Baseline Requirements for Code Signing") published at www.cabforum.org. If a discrepancy arises between interpretations of this document and the Requirements, the Requirements shall take precedence over this document. Additional assertions on standards used in this CPS can be found under the "Acknowledgements" section on the previous page.

This CPS addresses the technical, procedural and personnel policies and practices of GlobalSign during the complete lifecycle of Certificates issued by GlobalSign. GlobalSign operates within the scope of activities of GlobalSign NV. This CPS addresses the requirements of the CA that issues Certificates of various types. The chaining to any particular Root CA may well vary depending on the choice of intermediate Certificate and Cross Certificate used or provided by a platform or client.

This CPS is final and binding between GlobalSign nv/sa, a company under public law, with registered office at Diestsevest 14, 3000 Leuven, VAT Registration Number BE 0459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (hereinafter referred to as "GlobalSign"), 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 CPS.

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

1.1 Overview

This CPS applies to the complete hierarchy of Certificates issued by GlobalSign. The purpose of this CPS is to present the GlobalSign practices and procedures in managing Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to GlobalSign's own and industry requirements pursuant to the standards set out above. Additionally, eIDAS Regulation (Regulation (EU)N910/2014) provides for the recognition of electronic signatures that are used for the purposes of authentication or non-repudiation/contentCommitment. In this regard, GlobalSign operates within the scope of the applicable sections of the Law when delivering its services. This CPS aims to document GlobalSign's delivery of certification services and

management of the Certificate lifecycle of any issued Subordinate CA, client, server and other purpose end entity Certificates. The Certificate types addressed in this CPS are the following:

PersonalSign 1	A personal Certificate of low assurance
PersonalSign 2	A personal Certificate of medium assurance
PersonalSign 2 Pro	A personal Certificate of medium assurance with reference to professional context
PersonalSign 2 Pro DepartmentSign	A machine, device, department, or role Certificate of medium assurance with reference to professional context
PersonalSign 3 Pro	A personal Certificate of high assurance with reference to professional context
PersonalSign Partners	A private Certification Authority created as a trust anchor issuing PersonalSign 2 Pro or PersonalSign 2 Pro DepartmentSign
Noble Energy	A machine, device, department, or role Certificate of medium assurance with reference to professional context
IntranetSSL	A Certificate to authenticate web servers which does not chain to a publicly trusted GlobalSign Root
DomainSSL	A Certificate to authenticate web servers
AlphaSSL	A Certificate to authenticate web servers
OrganizationSSL & ICPEdu	A Certificate to authenticate web servers
ExtendedSSL[1]	A Certificate to authenticate web servers
GlobalSign Timestamping	A Certificate to authenticate time sources
AATL	A Certificate of medium hardware assurance for use with Adobe AATL and Microsoft Office documents
Code Signing[2]	A Certificate to authenticate data objects
Extended Validation Code Signing[1]	A Certificate to authenticate data objects
North American Energy Standard Board (NAESB) Authorized CA Certificates	A personal, role, server or device Certificate of either rudimentary, basic, or medium, with reference to professional context authorized by an Authorized Certification Authority
PDF Signing for Adobe CDS[3]	A Certificate of medium hardware assurance chained to the Adobe Root CA which may have reference to a professional context.
PersonalSign for Adobe CDS	A Certificate issued to natural persons (individuals) without a professional context in affiliation with an organization for the purpose of signing Adobe PDF documents.
PersonalSign Pro for Adobe CDS	A personal digital ID issued with reference to professional context for the purpose of signing Adobe PDF documents
DepartmentSign for Adobe CDS	A role-based certificate with reference to professional context for the purpose of signing Adobe PDF documents
Intermediate signing for Adobe/AATL	An intermediate CA that enters the GlobalSign hierarchy.
Timestamping for Adobe CDS	A Certificate to authenticate time sources
Test Digital Certificate for Adobe CDS	A Certificate for test or demonstration purposes which does not require hardware Assurance
Hosted Root	A service whereby GlobalSign maintains a Root Key and Certificate on behalf of a non GlobalSign entity and in parallel provides a cross certificate until such time as the Root has been embedded into Root stores. The non GlobalSign entity procures a WebTrust audit in their name during this period.
Qualified Certificates for Electronic Signatures	eIDAS compliant qualified certificates used for providing electronic signatures

[1] *These Certificates are issued and managed in accordance with the CA/Browser Forum EV Guidelines and EV Code Signing Guidelines. The remaining Certificate types shall be issued and managed in accordance with the Baseline Requirements if so, indicated by the inclusion of CA/Browser Forum Policy OIDs as detailed in Section 1.2 below.*

[2] *These Certificates are issued and managed in accordance with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.*

[3] *These Certificates are issued and managed in accordance with the Adobe Systems Incorporated Certificate Policy at http://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf*

Qualified Certificates for Electronic Seals	eIDAS compliant qualified certificates used for providing Electronic Seals
Qualified Web Authentication Certificates	eIDAS compliant qualified certificates for web authentication (SSL)
Certificates for Qualified Timestamping	Certificates used for signing eIDAS compliant qualified time stamps

GlobalSign Certificates:

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

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

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

This CPS states *"how the Certification Authority adheres to the Certificate Policy."* In doing so, this CPS features a greater amount of detail and provides the end user with an overview of the processes, procedures and conditions that GlobalSign uses in creating and maintaining the Certificates that it manages. In addition to the CP and CPS, GlobalSign maintains additional documented polices addressing such issues as:

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

Additionally, other relevant documents include:

- The GlobalSign Warranty Policy that addresses issues on warranties offered by GlobalSign;
- The GlobalSign Privacy Policy on the protection of personal data; and
- The GlobalSign Certificate Policy that addresses the trust objectives for the GlobalSign Root Certificates.

A Subscriber or Relying Party of a GlobalSign Issuing CA Certificate must refer to this CPS 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 CPS.

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

1.1.1 Certificate Naming

The exact names of the GlobalSign Root CA Certificates that are governed by this CPS are:

GlobalSign Public Root CA Certificates

- GlobalSign Root CA – R1 with serial number 040000000001154b5ac394
- GlobalSign Root CA – R3 with serial number 04000000000121585308a2
- GlobalSign Root CA – R5 with serial number 605949e0262ebb55f90a778a71f94ad86c
- GlobalSign Root CA – R6 with serial number 45e6bb038333c3856548e6ff4551
- GlobalSign Root CA – R7 with serial number 481b6a06a6233b90a629e6d722d5
- GlobalSign Root CA – R8 with serial number 481b6a09f4f960713afe81cc86dd
- GlobalSign Root CA – R46 with serial number 11d2bbb9d723189e405f0a9d2dd0df2567d1
- GlobalSign Root CA – E46 with serial number 11d2bbba336ed4bce62468c50d841d98e843

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

GlobalSign Non-TLS Root CA Certificates

- GlobalSign Client Authentication Root R45 with serial number 7653FEA649DAED25FEB4DFDAF7672535
- GlobalSign Client Authentication Root E45 with serial number 7653FEA6972D9953111D08449E0EB258
- GlobalSign Code Signing Root R45 with serial number 7653FE959602AB771F4CACCCF0AA020C
- GlobalSign Code Signing Root E45 with serial number 7653FE973CAA3B3FFD5E89FA976E6A1F
- GlobalSign Document Signing Root R45 with serial number 7653FE9ABF40624A8D61779A5A8DF848
- GlobalSign Document Signing Root E45 with serial number 7653FE9ECA542DDE2D54C38EEF180561
- GlobalSign Secure Mail Root R45 with serial number 7653FE912A5B2E0C629443130A570125
- GlobalSign Secure Mail Root E45 with serial number 7653FE93476C5E1C814784130052317D
- GlobalSign Timestamping Root R45 with serial number 7653FEA3DF6810924D16D9029562527F
- GlobalSign IoT Root R60 with serial number 7653FEA0C5E7F331B0DFF4B18A0C997D
- GlobalSign IoT Root E60 with serial number 7653FE93476C5E1C814784130052317D

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

Non-public Root Certificates

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

1.1.1.1 Public Disclosure of Subordinate Issuing CA Certificates

Browser root programs require that all Subordinate CAs that are not technically constrained (using Name Constraints and Extended Key Usage Constraints) are publicly disclosed. All "Active" Subordinate CA Certificates which chain directly or transiently to any Public Root CA certificate (R1, R3, R5, R6, R7, R8, R46, E46) are listed in the Common CA Database (CCADB). Deprecated Certificates that are not revoked are reported on a semi-annual basis to root programs via bugs or e-mails as required by the applicable root program. Revoked Subordinate CA certificates are also reported in the same manner, either shortly after revocation if routine or immediately after for a security concern.

Trusted Root is a GlobalSign service, which allows third party Issuing CAs to chain to one of the GlobalSign Root Certificates via an intermediate CA. Trusted Root end entity Certificates are outside the scope of this CPS as they are covered by the CPS of the third party.

- GlobalSign Trusted Platform Module Root CA with s/n 040000000000120190919AE
- GlobalSign Trusted Platform Module ECC Root CA with s/n 45dc9c8c1515db59d0464b9d79e9[4]

Trusted Root TPM is the GlobalSign service which allows third party Issuer CAs to chain to one of the GlobalSign Trusted Platform Module Root CA Certificates above and again, end entity Certificates are outside the scope of this CPS.

Certificates allow entities that participate in an electronic transaction to prove their identity to other participants or sign data digitally. By means of a Certificate, GlobalSign provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. The process to obtain a Certificate includes the identification, naming, authentication and registration of the Subscriber as well as aspects of Certificate management such as the issuance, revocation and expiration of the Certificate. By means of this procedure to issue Certificates, GlobalSign provides confirmation of the identity of the Subject of a Certificate by binding the Public Key the Subscriber uses through the issuance of a Certificate. GlobalSign makes available Certificates that can be used for non-repudiation/contentCommitment, encryption and authentication. The use of these Certificates can be further limited to a specific business or contractual context or transaction level in support of a warranty policy or other limitations imposed by the applications in which Certificates are used.

1.2 Document Name and Identification

This document is the GlobalSign Certification Practice Statement. The OID for GlobalSign nv-sa (the GlobalSign) is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign nv-sa (4146). GlobalSign organizes its OID arcs for the various Certificates and documents described in this CPS as follows:

Extended Validation	
1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy – SSL
1.3.6.1.4.1.4146.1.1.1	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC)
1.3.6.1.4.1.4146.1.1.2	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) – PSD2
1.3.6.1.4.1.4146.1.2	Extended Validation Certificates Policy – Code Signing
Domain Validation	
1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy
1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificates Policy – AlphaSSL
Organization Validation	
1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy
Intranet Validation	
1.3.6.1.4.1.4146.1.25	IntranetSSL Validation Certificates Policy
Timestamping	
1.3.6.1.4.1.4146.1.30	Timestamping Certificates Policy
1.3.6.1.4.1.4146.1.31	Timestamping Certificates Policy – AATL
1.3.6.1.4.1.4146.1.32	Timestamping Certificate Policy – Certificates for Qualified Time Stamping (QTS) under eIDAS regulation
1.3.6.1.4.1.4146.2	Policy by which the timestamping services operated by GlobalSign incorporates the time into IETF RFC 3161 responses
1.3.6.1.4.1.4146.2.1	CDS Timestamp Test Policy

[4] *Collectively Root R1, R3, R5, R6, R7, R8, R46, E46 and the TPM/TPM ECC Roots are referred to as the GlobalSign Root Certificates.*

1.3.6.1.4.1.4146.2.2	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 1 (SHA1)
1.3.6.1.4.1.4146.2.3	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2)
1.3.6.1.4.1.4146.2.4	RFC3161 Timestamp Test Policy ECC
1.3.6.1.4.1.4146.2.5	Qualified Timestamping Tokens for eIDAS

Client Certificates

1.3.6.1.4.1.4146.1.40	Client Certificates Policy (Generic)
1.3.6.1.4.1.4146.1.40.10	Client Certificates Policy (EPKI – Enterprise PKI)
1.3.6.1.4.1.4146.1.40.20	Client Certificates Policy (JCAN – Japan CA Network)
1.3.6.1.4.1.4146.1.40.30	Client Certificates Policy (AATL)
1.3.6.1.4.1.4146.1.40.40	Client Certificates Policy (EPKI for private CAs)
1.3.6.1.4.1.4146.1.40.50	Client Certificates Policy (Private Hierarchy)

Qualified Certificates under eIDAS

1.3.6.1.4.1.4146.1.40.35	eIDAS Qualified Certificates (Generic)
1.3.6.1.4.1.4146.1.40.35.1	Qualified Certificates for Electronic Seals (Legal Persons)
1.3.6.1.4.1.4146.1.40.35.1.1	Qualified Certificates for Electronic Seals (Legal Persons) - PSD2
1.3.6.1.4.1.4146.1.40.35.2	Qualified Certificates for Electronic Signatures (Natural Persons)

In addition to these identifiers, all Certificates that comply with the itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2) will include the following additional identifier:

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 (maps to 1.3.6.1.4.1.4146.1.40.35.2)
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 (maps to 1.3.6.1.4.1.4146.1.40.35.1)

Code Signing

2.23.140.1.4.1	Code Signing Minimum Requirements Policy
1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy

Certificates issued by GlobalSign containing 1.3.6.1.4.1.4146.1.50 are issued and managed in accordance with the Baseline Requirements for Code Signing.

CA Chaining and Cross Signing

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

Others

1.3.6.1.4.1.4146.1.26	Test Certificate Policy – Should not be trusted as it may not contain accurate information. This is to be used for testing and integration purposes.
1.3.6.1.4.1.4146.1.70	High Volume CA Policy
1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90	Trusted Root TPM Policy
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy

1.3.6.1.4.1.4146.3	GlobalSign's documents (such as Certificate Policy (CP) and Certification Practice Statement (CPS))
1.3.6.1.4.1.4146.4	GlobalSign-specific certificate extensions
1.2.840.10045.4.1	ECDSAWithSHA1
1.2.840.10045.4.3.1	ECDSAWithSHA224
1.2.840.10045.4.3.2	ECDSAWithSH256
1.2.840.10045.4.3.3	ECDSAWithSHA384
1.2.840.10045.4.3.4	ECDSAWithSHA512

Internet of Things (IoT)

1.3.6.1.4.1.4146.1.100	Internet of Things Device Certificates Policy

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

2.16.840.1.114505.1.12.1.2	NAESB Rudimentary Assurance
2.16.840.1.114505.1.12.2.2	NAESB Basic Assurance
2.16.840.1.114505.1.12.3.2	NAESB Medium Assurance

In addition to these identifiers, all Certificates that comply with the Baseline Requirements will include the following additional identifiers:

2.23.140.1.1	Extended Validation Certificate Policy
2.23.140.1.2.1	Domain Validation Certificates Policy
2.23.140.1.2.2	Organization Validation Certificates Policy

1.3 PKI Participants

1.3.1 Certification Authorities

GlobalSign is a Certification Authority that issues Certificates in accordance with this CPS. As a Certification Authority, GlobalSign performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. GlobalSign also provides Certificate status information using a Repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder. A Certification Authority may also be described by the term *"Issuing Authority"* or *"GlobalSign"* to denote the purpose of issuing Certificates at the request of a Registration Authority (RA) from a subordinate Issuing CA.

The GlobalSign PACOM1 - CA Governance Policy Authority, which is composed of members of the GlobalSign management team and appointed by its Board of Directors, is responsible for maintaining this CPS relating to all Certificates in the GlobalSign hierarchy. Through its Policy Authority, GlobalSign has ultimate control over the lifecycle and management of the GlobalSign Root CA and any subsequent subordinate Issuing CAs including Trusted Root Issuing CAs belonging to the hierarchy.

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

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

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

1.3.2 Registration Authorities

In addition to identifying and authenticating Applicants for Certificates, a Registration Authority (RA) may also initiate or pass along revocation requests for Certificates and requests for reissuance and

renewal (sometimes referred to as re-key) of Certificates. GlobalSign may act as a Registration Authority for Certificates it issues in which case GlobalSign is responsible for:

- Accepting, evaluating, approving or rejecting the registration of Certificate applications;
- Registering Subscribers for certification services;
- Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);
- Using officially notarised or otherwise authorised documents or sources of information to evaluate and authenticate an Applicant's application;
- Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and
- Initiating the process to revoke a Certificate from the applicable GlobalSign subordinate Issuing CA or partner Subordinate CA.

Third party Issuing CAs who enter into a contractual relationship with GlobalSign may operate their own RA and authorize the issuance of Certificates. Third parties must comply with all the requirements of this CPS and the terms of their contract which may also incorporate additional criteria as recommended by the CA/B Forum and/or browser root programs. RAs may implement more restrictive vetting practices if their internal policy dictates.

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

In the case of EPKI (Enterprise PKI) and MSSL (Managed SSL) RAs, certificates are constrained by a pre-defined and validated GlobalSign configuration.

GlobalSign may designate an Enterprise RA to verify Certificate Requests from the Enterprise RA's own organization. EPKI (Enterprise PKI) and MSSL (Managed SSL) utilize Enterprise RA, where the Subscriber's organization is validated and pre-defined, and are constrained by GlobalSign system configuration. For an Enterprise RA to represent the organization, the following requirements are validated by GlobalSign:

1. Requested FQDN are within the Enterprise RA's verified Domain Namespace; and
2. If the Certificate Request includes a Subject name of a type other than FQDN, GlobalSign confirms that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject.

1.3.2.1 RA specific requirements for ExtendedSSL and Extended Validation Code Signing Certificates

For the issuance of ExtendedSSL and Extended Validation (EV) Code Signing Certificates, GlobalSign contractually obligates each RA and/or subcontractor to comply with all applicable requirements in the EV Guidelines and EV Code Signing Guidelines, as applicable.

Under the terms of the EV Guidelines, GlobalSign may contractually authorize the Subject of a specified valid EV Certificate to perform the RA function and authorize GlobalSign to issue additional EV Certificates at third and higher domain levels that contain the Domain Name that was included in the original EV Certificate (also known as "Enterprise EV Certificates"). In such case, the Subject shall be considered an Enterprise RA, and shall not authorize the CA to issue any ExtendedSSL Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA.

GlobalSign shall not delegate the performance of the final cross-correlation and due diligence requirements of Section 11.12 of the EV Guidelines.

1.3.2.2 RA-Specific Requirements for Qualified Certificates

GlobalSign MAY delegate the verification of both the Organization Identity and the Individual Identity to a Registration Authority under the condition that this Registration Authority meet the verification requirements as set by eIDAS Regulation.

This condition is considered to be met in the following scenarios:

- The Delegated Registration Authority passes an audit to confirm that the Subscriber information is properly authenticated, following the relevant "Verification" sections in GlobalSign's CP and CPS for Qualified Certificates for Electronic Signatures.
    - GlobalSign shall monitor adherence to its Certificate Policy and CPS by the delegated Local Registration Authority by performing ongoing quarterly audits against a randomly selected sample of at least the greater of one (1) certificate or one percent (1%) of the Qualified Certificates verified by delegated Local Registration Authority in the period beginning immediately after the last sample was taken.
- The Registration Authority provides GlobalSign with an audit report equivalent to a conformity assessment report. The equivalence to the conformity assessment report will be confirmed by a Conformity Assessment Body (as defined in eIDAS Regulation) prior to the acceptance by GlobalSign. In the evaluation, the Conformity Assessment Body will consider:
    - The equivalence to the eIDAS requirements of the requirements that the Registration Authority;
    - The scope and the conclusions of the audit.

Most organizations will perform an in-person (or equivalent) identification of their employees, agents or contractors. These organizations may act as a Registration Authority for GlobalSign with regards to the identity verification of their employees, contractors or agents. In this case, there will be an agreement between GlobalSign and the organization, and GlobalSign will perform a security assessment of employee identification procedures. Certificates issued using this specific Registration Authority type contain the organization information in the Certificate, and may only be used for the employment purposes.

1.3.3 Subscribers

Subscribers are either Legal Entities or natural persons that successfully apply for and receive a Certificate to support their use in transactions, communications and the application of Digital Signatures.

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

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

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

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

It is expected that a Subscriber organization has a service agreement or other pre-existing contractual relationship with GlobalSign authorising it to carry out a specific function within the scope of an application that uses GlobalSign Certificate services. Issuance of a Certificate to a

Subscriber organization is only permitted pursuant to such an agreement between GlobalSign and the subscribing end entity.

1.3.4 Relying Parties

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

Adobe offers the AATL platform from Acrobat® 9.12 and above in order to provide document recipients with improved assurances that certified PDF documents are authentic. Document recipients are Relying Parties who use Adobe products on supported platforms to verify the Subscriber's signature on a certified PDF document. It is best practice for certifying authors to include Certificate status information and an appropriate timestamp within a signed PDF. Such additional detail may be inspected by Relying Parties by using a suitable version of the Adobe PDF reader.

1.3.5 Other Participants

Other participants include bridge CAs and CAs that cross certify Issuing CAs to provide trust among other PKI communities. For example, the GlobalSign Root R1, R3, R5 and R6 are cross certified by Microsoft Code Verification Root to allow provision of kernel mode drivers including support in Windows 10. These Cross Certificates name GlobalSign as the Subject and are listed below.

Note that the cross Certificate to R1 can also be downloaded from the Microsoft Web Site here. GlobalSign's support pages will detail which cross certificate is appropriate to which product offering.

Microsoft Code Signing Cross Certificate to R1

-----BEGIN CERTIFICATE-----
MIIFJjCCAw6gAwIBAgIKYSkVJwAAAAAAKjANBgkqhkiG9w0BAQUFADB/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHUmVkbW9uZDEe
MBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQDEyBNaWNyb3Nv
ZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xMTA0MTUxOTU1MDhaFw0yMTA0
MTUyMDA1MDhaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52
LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxTaWduIFJvb3Qg
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZjc6j40+Kfvvx
i4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavpxy0Sy6scTHAH
oT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp1Wrjsok6Vjk4
bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdGsnUOhugZitVt
bNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJU26Qzns3dLlw
R5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N89iFo7+ryUp9/
k5DPAgMBAAGjgcswgcgwEQYDVR0gBAowCDAGBgRVHSAAMAsGA1UdDwQEAwIBhjAP
BgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzAf
BgNVHSMEGDAWgBRi+wohW39DbhHaCVRQa/XSlnHxnjBVBgNVHR8ETjBMMEqgSKBG
hkRodHRwOi8vY3JsLm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNy
b3NvZnRDb2RlVmVyaWZSb290LmNybDANBgkqhkiG9w0BAQUFAAOCAgEAX/jQZXRq
gcamylsDtpFK6Eu97yuhQvDvtKWtzTOJ7AuVhaxiUBEIqljSWqCDEOWmM3ryWvLF
/nh88JyD3xkK2XOWAC3WLM3pFNQdneg/PBp295BO+wE1CmyTE6DDVutnoOTRepbe
wmfxkPgKe/UyG5TsX3UfjRs02mxYp8stJ54iJrfJqjDMB3e4NuOCAbU5PMyN2adf
fyOzh3/bV5iRi9fOJSDjnWRP3Yf3K2hJAxjgpd98X2hkTTaDjUeB8ungqGmr+nsW
PAWkSeqIMBkKbHMFUXjf1B3dOtR/LeROVL6DQx56dDO0pOvXcHO8KgKYiWbu9ryP
dJN44ykCWlpD4ljOfM+aytI2iTviX9omBU7I1OcskQ4Xl8W+7osTESMjKU/6g9BQ
9rr61T2zFz30/wNKoyXc5nVh0fo1CGvWJ0TQaLeNReDrhSzIoV1hRHQWDllYrtK1
7qW81tcHarYpeP2XZ2fdjU8XlE/S7QyvlyQ3w6Kcgdpr4UO2V3tM7L95Exnnn+hE
6UeBt15wHpH4PdF7J/ULcFZDSAXdqS+rhhAdCxLjGtBMbnXe1kWzC3SIh5NcVkpB
Apr3rreZ2LZ/iPoR8kV89NcbkcAc8aD71AgKQRoUKs706zRIbmaHntVLejl/uw49
OGHPc1cG5BIGa9lrUwjNcBjCLU+XRpG8qfA=
-----END CERTIFICATE-----

Microsoft Code Signing Cross Certificate to R3

-----BEGIN CERTIFICATE-----
MIIFKTCCAxGgAwIBAgITMwAAADtqwB4rIeYV3AAAAAAAOzANBgkqhkiG9w0BAQUF
ADB/MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMH
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQD
EyBNaWNyb3NvZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xNTA2MDQxNzQ3
NTNaFw0yNTA2MDQxNzQ3NTNaMEwxEzARBgNVBAoTCkdsb2JhbFNpZ24xIDAeBgNV
BAsTF0dsb2JhbFNpZ24gUm9vdCBDQSAtIFIzMRMwEQYDVQQDEwpHbG9iYWxTaWdu
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzCV2kHkGeCIW9cCDtoTK

KJ79BXYRxa2IcvxGAkPHsoqdBF8kyy5L4WCCRuFSqwyBR3Bs3WTR6/Usow+CPQwr
rpfXthSGEHm7OxOAd4wI4UnSamIvH176lmjfiSeVOJ8G1z7JyyZZDXPesMjpJg6D
FcbvW4vSBGDKSaYo9mk79svIKJHlnYphVzesdBTcdOA67nIvLpz70Lu/9T0A4QYz
6IIrrlOmOhZzjN1BDiA6wLSnoemyT5AuMmDpV8u5BJJoaOU4JmB1sp93/5EU764g
SfytQBVI0QIxYRleuJfvrXe3ZJp6v1/BE++bYvsNbOBUaRapA9pu6YOTcXbGaYWC
FwIDAQABo4HQMIHNMBMGA1UdJQQMMAoGCCsGAQUFBwMDMBIGA1UdEwEB/wQIMAYB
Af8CAQEwCwYDVR0PBAQDAgGGMB0GA1UdDgQWBBSP8Et/qC5FJK5NUPpjmove4t0b
vDAfBgNVHSMEGDAWgBRi+wohW39DbhHaCVRQa/XSlnHxnjBVBgNVHR8ETjBMMEqg
SKBGhkRodHRwOi8vY3JsLm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9N
aWNyb3NvZnRDb2RlVmVyaWZSb290LmNybDANBgkqhkiG9w0BAQUFAAOCAgEAYAKs
DgkNtGp9WQytZkUKGA9epyVcFPbTWs+dXjvHevwAX25AKy3hzm92qzyr2flFz3eQ
UuohlzrSXT5XunPsAHV3onVFdMdiJrBUutXJydps7Wby/4sXsnlZyoBUZdqWyhHe
KrvD1D03/Ob9y5KGbrmtTRto4EfZsIY0IxzaHd1uVO3LDuF61U2yoavO2nEvoj4I
BKwqU9cT2TxuM4ynt7k1r6VZ3zBf6j7od3Ej+PnpHtviFANqiu9kwXvgXVbg5PLI
TODX7wfT1iD63mUZmKfGcStdlK7pyQuRV4aQzN6f1DwZlQQ+/VwrpPw5lY+oh4ey
W8qAT8MWOPUOsO3Xyvb8d0R32ErInZ//MBeY1xLVkN3lOmbg8SyXR5m2Dw5W2ptB
DcNL1fBonMqlhlyGZhLyO4ME/0btLWTUVpUrfnmdAYMTGNVovZHO3Yb7CKCrDEVk
w9EmNF5WomxMaQyLY8qEGHrFc6uzUq6N3OIrA2d9hioSb2hPZIF1LYXluOyABZur
OWnuHzFqair7Nb1jqsXuZdPWlqQ+mZMevu47bGRsrs0UCvzYjCCjHPhif6TAfR8s
fzpQwCaTljecj6UTY7Rz2BarJ0h+qv7rD0h/KZieO0mRkPCPPrrcnyaBnXNmMacn
tuSpTQTl6lMxwPqTSoed/Eph4GOirE+I9MV4H2U=
-----END CERTIFICATE-----

Microsoft Code Signing Cross Certificate to R5

-----BEGIN CERTIFICATE-----
MIIEfzCCAmegAwIBAgITMwAAADxDRdim0Drf5AAAAAAAPDANBgkqhkiG9w0BAQUF
ADB/MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMH
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQD
EyBNaWNyb3NvZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xNTA2MDQxNzQ3
NTRaFw0yNTA2MDQxNzQ3NTRaMFAxEzARBgNVBAoTCkdsb2JhbFNpZ24xJDAiBgNV
BAsTG0dsb2JhbFNpZ24gRUNDIFJvb3QgQ0EgLSBSNTETMBEGA1UEAxMKR2xvYmFs
U2lnbjB2MBAGByqGSM49AgEGBSuBBAAiA2IABEdFDpb7fV2/6TnRIfifC7bVex6S
OkhZHPBiMS3Aeij+Gqdcs7bMl+dF1Fj60XdtQ6LAh2U0Ch963es8M6HFnU2kb0GV
OH/JHoTr0Z5JkoeUhww6hUpmn51Zk02XYQaGSqOB0DCBzTATBgNVHSUEDDAKBggr
BgEFBQcDAzASBgNVHRMBAf8ECDAGAQH/AgEBMAsGA1UdDwQEAwIBhjAdBgNVHQ4E
FgQUPeYpSJvqB8ohREom3m7e0oPQn1kwHwYDVR0jBBgwFoAUYvsKIVt/Q24R2glU
UGv10pZx8Z4wVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL2NybC5taWNyb3NvZnQu
Y29tL3BraS9jcmwvcHJvZHVjdHMvTWljcm9zb2Z0Q29kZVZlcmlmUm9vdC5jcmww
DQYJKoZIhvcNAQEFBQADggIBAEAHoOGyvU9GfLBcmnCnTFGXBNCEJiW3f3ENX+9L
/fsgNlPL3XsnL8/tzNvS8GccIxAPMjsOwaEX2wZuImSq3J9SqVhOksgovkDR0lTp
jd7PPz9s65rvnGfEWa2BE3vRCiDSBvGtA/EnSdodZKS7RFlfMNoke2oS5E1oKpl1
OeTmZTnZv4WW76WcOrIpY1+or2/ci9z9J8fGETyVVZb2t6yaBN3lMVo7yR9JyNjv
WaOtC19QKW28YGaci9zg9JmRaWXQ6eOOX2o+tZaO5mwtdqqHls4StRPb44f4MPtK
k8Jw9IjcLcagpFelYDJTLtKFHmDwdTd1go7DJjZixaiCugqBiEJ3NFXq9EzX4lIa
6kdWw26haxtVLmG23DTfPlqWahlB2joMeJtLIirh4Jk2PS4viF69PRAb54m1bIYx
EiUPuw07tzXowHh+e5vvwnLCFvaas6w6pILcPYJ0MOvB2/EAji6GcpVGtmnMBEiG
/sSbLq7V+FhN9h8g/RipSZDpW0G760Rr1gInXQZyvaFpVO9kfV1DSnCDC+aVzZbO
3NoFAEJV4p3SnAnQJ3J7SqdBIV5hMGhxFeuGWV/fQL0jkvG162LS+PRwAccvhSVV
i69OcMgjPcqUeg6QQ8ikJ7+wl27BSD/cTD9Rj0DtVRN/G5VxgBLF2gEFNgmOemup
DwgW
-----END CERTIFICATE-----

Microsoft Code Signing Cross Certificate to R6

-----BEGIN CERTIFICATE-----
MIIGKTCCBBGgAwIBAgITMwAAAD3vOO4dp2hzYQAAAAAAPTANBgkqhkiG9w0BAQUF
ADB/MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMH
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQD
EyBNaWNyb3NvZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xNTA2MDQxNzQ3
NTRaFw0yNTA2MDQxNzQ3NTRaMEwxEzARBgNVBAoTCkdsb2JhbFNpZ24xIDAeBgNV
BAsTF0dsb2JhbFNpZ24gUm9vdCBDQSAtIFI2MRMwEQYDVQQDEwpHbG9iYWxTaWdu
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAlQfoc8pm+ewUyns89w0I
8bRFCyyCtEjG61s8roO4QZIzFKRvf+kqzMawiGvFtonRxrL/FM5RFCHsSt0bWsbW
h+5NOhUG7WRmC5KAykTec5RO86eJf094YwjIElBtQmYvTbl5KE1SGooagLcZgQ5+
xIq8ZEwhHENo1z08isWyZtWQmrcxBsW+4m0yBqYe+bnrqqO4v76CY1DQ8BiJ3+QP
efXqoh8q0nAue+e8k7ttU+JIfIwQBzj/ZrJ3YX7g6ow8qrSk9vOVShIHbf2MsonP
0KBhd8hYdLDUIzr3XTrKotudCd5dRC2Q8YHNV5L6frxQBGM032uTGL5rNrI55Kwk
Nrfw77YcE1eTtt6y+OKFt3OiuDWqRfLgnTahb1SK8XJWbi6IxVFCRBWU7qPFOJab
Tk5aC0fzBjZJdzC8cTflpuwhCHX85mEWP3fV2ZGXhAps1AJNdMAU7f05+4PyXhSh
BLAL6f7uj+FuC7IIs2FmCWqxBjplllnA8DX9ydoojRoRh3CBCqiadR2eOoYFAJ7b
gNYl+dwFnidZTHY5W+r5paHYgw/R/98wEfmFzzNI9cptZBQselhP00sIScWVZBpj
Dnk99bOMylitnEJFeW4OhxlcVLFltr+Mm9wT6Q1vuC7cZ27JixG1hBSKABlwg3mR
l5HUGie/Nx4yB9gUYzwoTK8CAwEAAaOB0DCBzTATBgNVHSUEDDAKBggrBgEFBQcD

AzASBgNVHRMBAf8ECDAGAQH/AgEBMAsGA1UdDwQEAwIBhjAdBgNVHQ4EFgQUrmwF
o5MT4qLn4tcc1sfwf8hnU6AwHwYDVR0jBBgwFoAUYvsKIVt/Q24R2glUUGv10pZx
8Z4wVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL2NybC5taWNyb3NvZnQuY29tL3Br
aS9jcmwvcHJvZHVjdHMvTWljcm9zb2Z0Q29kZVZlcmlmUm9vdC5jcmwwDQYJKoZI
hvcNAQEFBQADggIBAKxHC181ziPmhqUOo5FlccJjaiLqIaHvwyvfWNnkaH8oYTpz
4VpkWA1Jf0ULvL875Lt/mS6Nl5Lt1RuOscQQdLqCgJdYThdbvDmBrX6SfZUd0r98
qIKXuRq2rSLhzLNrN6y//W8B94iVIT2AfuyJOTrMKHhiFOAkWqnclj/4kzV+fJVr
DStpFYhXanXKm9h+IVzsY//VuTDqei1aubVRcTXqWKRzn0keTlVTOKekfzSatpif
JFmtbjyvssL1hMH0ga/BtxLUp6c7Ls7vRV9qB3ZwT9jafhbD1qQgqc/X2S7H+eQr
cfhQ+EIAK2YiZLjvGX3zyRppuYzPiVjD9NFV6XcUf352AcB/pRZYXp4bMLniLK+a
LvksFG/g+e8+97kIUWmIintUe9ivQdnPeFEC/5AVHZaKfdAJOp9oqB/3WRbK+Cq4
Q3+3nb/5JiNVmAeDYoKOMXtAO0q5PWHL3ilBCQPtXcQ/bdShoPCfTHrWy7iO7m7K
BGrLFeHbxQucW10YbRAWnQ4s3Z5qMvFStcFAV+QUOofwEUrqJASZ0/Rvy7RrmHev
X8PKasM+CInaQiZxdsBCZ3il8hK2sEZTFhtxCzJ9p8dgu/K7SB0oEgfyL2+4NRAv
vMRAolNctIQjPS5g5RSPTvoyXMvKxPubaC+3MhDsftQoo/yCeHAsMY+Rw3T6
-----END CERTIFICATE-----

1.4 Certificate Usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate Certificate Usage

End entity Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Certificates issued by GlobalSign can be used for public domain transactions that require:

- **Non-repudiation/contentCommitment** A party cannot deny having engaged in the transaction or having sent the electronic message.
- **Authentication** The assurance to one entity that another entity is who he/she/it claims to be.
- **Confidentiality (Privacy)** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- **Integrity** The assurance to an entity that data has not been altered (intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt.

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

- **PersonalSign 2** Non-repudiation/contentCommitment of a transaction (medium level assurance)
- **PersonalSign 2/3 Pro** Non-repudiation/contentCommitment of the transaction by a party acting in an organizational context (medium level assurance)
- **Noble Energy** Non-repudiation/contentCommitment of the transaction by a party acting in an organizational context (medium level assurance)
- **AATL** Non-repudiation/contentCommitment of the transaction by a party acting in an organizational context (medium hardware level assurance). (It is not recommended that the Certificate be used for encryption due to the singularity of the Certificate and inability to provide key escrow services under the Adobe Certificate Policy.)
- **Qualified Certificates** Non-repudiation/contentCommitment of signatures by Individuals (Qualified Certificates for Electronic Signatures) and legal persons (Qualified Certificates for Electronic Seals)

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

- **PersonalSign 2** Authentication of a natural person (medium level assurance) and the existence of an email address
- **PersonalSign 2 Pro** Authentication of a natural person within an organizational context or a machine, device, department, or role within an organizational context (medium level assurance) and optionally the existence of an email address
- **Noble Energy** Authentication of a natural person within an organizational context or a machine, device, department, or role within an organizational context (medium level assurance) and optionally the existence of an email address
- **PersonalSign 3 Pro** Authentication of a natural person within an organizational context (high level assurance)
- **NAESB Rudimentary** Authentication as prescribed in NIST SP800-63A Digital Identity Guidelines: Enrollment and Identity Proofing, Section 4.3 "Identity Proofing Assurance Level I.
- **NAESB Basic** Authentication as prescribed in CA/Browser Forum Baseline Requirements for the issuance and management of Publicly Trusted Certificates. Section 3.2.3 Authentication of Individual Identity. Employers who verified the identity of their applicants by means comparable to those stated above for Basic Level may elect to become an LRA and perform identity proofing of applicants either in-person by inspection of its corporate issued photo ID or through the LRA's secure online process. The corporate issued photo ID or online process should originate with a government issued photo ID.
- **NAESB Medium** Authentication as prescribed in CA Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. Chapter 11.2.2: Acceptable Method of Verification (4) Principal Individual

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

- **DomainSSL** Authentication of a remote Domain Name and webservice and encryption of the communication channel
- **AlphaSSL** Authentication of a remote Domain Name and webservice and encryption of the communication channel
- **OrganizationSSL** Authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel
- **ICPEdu** Authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel
- **ExtendedSSL** Authentication of a remote domain name and associated organizational context and webservice and encryption of the communication channel
- **Code Signing** Authentication of a data object with a legal person or a Legal Entity
- **EV Code Signing** Authentication of a data object with a legal person or a Legal Entity
- **Timestamping** Authentication of a time and date related to a service within an organizational context
- **PersonalSign (All)** Authentication of device or machine associated with an organization
- **NAESB Rudimentary** Authentication as prescribed in NIST SP800-63 A Digital Identity Guidelines: Enrollment and Identity Proofing, Section 4.3 "Identity Proofing Assurance Level I.
- **NAESB Basic** Authentication as prescribed in CA/Browser Forum Baseline Requirements for the issuance and management of Publicly Trusted Certificates. Section 3.2.3 Authentication of Individual Identity.
- **NAESB Medium** Authentication as prescribed inBrowser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. Chapter 11.2.2: Acceptable Method of Verification (4) Principal Individual

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

- **Low assurance** (Class 1) Certificates are not suitable for identity verification as no authenticated identity information is included within the Certificate. These Certificates do not support non-repudiation/contentCommitment.
- **Medium assurance** (Class 2) Certificates are individual and organizational Certificates that are suitable for securing moderately risky inter and, intra-organizational, and commercial transactions.
- **High assurance** (Class 3) Certificates are individual and organizational Certificates that provide a high level of assurance of the identity of the Subject as compared to Class 1 and 2.
- **High assurance (EV)** Extended Validation Certificates are Class 3 Certificates issued by GlobalSign in conformance with the EV Guidelines.
- **NAESB Rudimentary** This level provides the lowest degree of assurance. One of the primary functions of this level is to provide data integrity of the information being signed. This level is appropriate for environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where Certificates having higher levels of assurance are unavailable.
- **NAESB Basic** This level provides a basic level of assurance appropriate for environments where there are risks and consequences of data Compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this assurance level that users are not likely to be malicious.
- **NAESB Medium** This level is appropriate for environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

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

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

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

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

1.4.2 Prohibited Certificate usage

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorised. Certificates are

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

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

Certificates issued under this CPS may not be used:

- For any application requiring fail safe performance
- Where prohibited by law
- Certificates for electronic signatures should only be used by natural persons whereas certificates for Electronic Seals should only be used by legal persons
- Certificates issued under the NAESB WEQ PKI shall never be used for performing either of the following functions:
    - Any transaction or data transfer that may result in imprisonment if compromised or falsified.
    - Any transaction or data transfer deemed illegal under federal law

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

PACOM1 – CA Governance GlobalSign NV
Diestsevest 14,
3000 Leuven, Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909

1.5.2 Contact Person

General Inquiries

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

Certificate Problem Report

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

report-abuse@globalsign.com

GlobalSign may or may not revoke in response to this request. See section 4.9.5 for detail of actions performed by GlobalSign for making this decision.

1.5.3 Person Determining CPS Suitability for the Policy

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

In an effort to maintain credibility and promote trust in this CPS and better correspond to accreditation and legal requirements, the PACOM1 – CA Governance shall review this CPS at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CPS.

1.5.4 CPS Approval Procedures

PACOM1 – CA Governance reviews and approves any changes to the CPS. The updated CPS is reviewed against the CP in order to check for consistency. CP changes are also added on an as-needed basis. Upon approval of a CPS update by PACOM1 – CA Governance, the new CPS is published in the GlobalSign Repository at https://www.globalsign.com/repository.

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

1.6 Definitions and Acronyms

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

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

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

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

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

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

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

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

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

CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

DNS CAA Email Contact: The email address defined in Appendix B.1.1. of the CA/B Forum Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Appendix B.2.1. of the CA/B Forum Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Appendix B.2.2. of the CA/B Forum Baseline Requirements.

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

Hash (e.g. SHA1 or SHA256): An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

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

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

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

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

Individual: A natural person.

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

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

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

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

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

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

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

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

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

North American Energy Standards Board (NAESB) Accreditation Requirements for Authorized Certification Authorities ("NAESB Accreditation Specification"): The technical and management details which a Certification Authority is required to meet in order to be accredited as an Authorized Certification Authority (ACA) by NAESB.

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

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

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

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

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

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

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

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

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

PSD2 Certificate: A Qualified Certificate that includes PSD2 Specific Attributes.

PSD2 Specific Attributes: Attributes that are specific to PSD2 Certificates which are:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Qualified Trust Service Provider (QTSP): A natural or legal person that is recognized by a European Union member state national supervisory body to provide (a subset of) qualified trust service as defined within the eIDAS Regulation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vetting Agent: Someone who performs the information verification duties specified by the Baseline Requirements.

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

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

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

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

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

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

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

AATL	Adobe Approved Trust List
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
CA	Certification Authority
CAA	Certificate Authority Authorization
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EIR	Electric Industry Registry
EKU	Extended Key Usage
EPKI	Enterprise PKI
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GCC	GlobalSign Certificate Center
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEduA	Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NAESB	North American Energy Standards Board

NCA	National Competent Authority
NIST	(US Government) National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PSP	Payment service provider
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax
WEQ	Wholesale Electric Quadrant

2.0 Publication and Repository Responsibilities

2.1 Repositories

GlobalSign publishes all CA Certificates and Cross Certificates, revocation data for issued Certificates, CP, CPS, and Relying Party agreements and Subscriber Agreements in Repositories. GlobalSign ensures that revocation data for issued Certificates and its Root Certificates are available through a Repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

GlobalSign may publish submitted information on publicly accessible directories for the provision of Certificate status information.

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

Country specific web sites and translations of this CPS and other public documentation may be made available by GlobalSign and/or group companies for marketing purposes, however the legal repository for all GlobalSign public facing documentation is https://www.globalsign.com/repository and in the event of any inconsistency, the English language version shall control.

2.2 Publication of Certificate Information

GlobalSign publishes its CP, CPS, Subscriber Agreements, and Relying Party agreements at https://www.globalsign.com/repository. The CP and CPS include all the material required by RFC 3647, and are structured in accordance with RFC 3647. CRLs are published in online repositories. The CRLs contain entries for all revoked unexpired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

GlobalSign hosts test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. Below are test Web pages for (i) valid, (ii) revoked, and (iii) expired certificates.

Root R1:

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

Root R3:

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

Root R5:

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

Root R6

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

Root R7

https://valid.r7.roots.globalsign.com
https://revoked.r7.roots.globalsign.com
https://expired.r7.roots.globalsign.com

Root R8

https://valid.r8.roots.globalsign.com
https://revoked.r8.roots.globalsign.com
https://expired.r8.roots.globalsign.com

Root R46

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

Root E46

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

2.3 Time or Frequency of Publication

CA Certificates are published in a Repository via support pages as soon as possible after issuance. CRLs for end entity Certificates are updated every 24 hours and are valid for 7 days. CRLs for CA Certificates are issued at least every 3 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

GlobalSign reviews its CP and CPS at least annually and makes appropriate changes so that GlobalSign operation remains accurate, transparent and complies with external requirements listed in the "*Acknowledgements*" section of this document. GlobalSign closely monitors CA/Browser Forum ballots and updates to the Requirements and implements updates to GlobalSign operations in a timely manner. New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after being digitally signed by the CPS PACOM1 - CA Governance using an Adobe AATL PDF signing Certificate with appropriate timestamp.

2.4 Access Controls on Repositories

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

Logical and physical security measures are implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3.0 Identification and Authentication

GlobalSign acts as an RA and verifies and authenticates the identity and/or other attributes of an Applicant prior to inclusion of those attributes in a Certificate.

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

GlobalSign RAs authenticate the requests of parties wishing to revoke Certificates.

3.1 Naming

3.1.1 Types of Names

GlobalSign Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading. However, some Certificates such as IntranetSSL SSL Common Names and/or GlobalSign may also include RFC2460 (IP version 6) or RFC791 (IP version 4) addresses.

Wildcard SSL Certificates include a wildcard asterisk character as the first character in a CN or SAN. Before issuing a Certificate with a wildcard character (*) in the CN or SAN, GlobalSign follows best practices to determine if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix.” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation.) and, if it does, it will reject the request if that Domain Namespace is not owned or controlled by the Subscriber.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

GlobalSign enforces the uniqueness of each Subject name in a Certificate as follows. For the definition of “Class” below, please see section 3.2.3.

- **PersonalSign1 Certificates** A unique email address only (Class 1).
- **PersonalSign Certificates** A unique email address and the name of an individual along with the name of the Country which issued the passport or equivalent credential the individual provides to prove their identity to GlobalSign (Class 2).

- **PersonalSign Pro Certificates** A unique email address (if to be included in the Certificate) coupled with an Organization name and optionally state and locality the Organization is registered at and either the name of an individual or Department and optionally Organization Unit affiliated with the Organization (Class 2)
- **PersonalSign 3 Pro Certificates** A unique email address coupled with an organization's name and state and/or locality and the name of an individual, as verified on the passport or equivalent credential the holder provides to prove their identity in person with either GlobalSign or a Trusted Third Party (Class 3).
- **Noble Energy Certificates** A unique email address (if to be included in the Certificate subjectDN) coupled with an organization's name and state and/or locality plus either the name of an individual or a department associated with the organization. (Class 2)
- **Code Signing Certificates** A unique organization name and state and/or locality or a unique individual name and state and/or locality with an optional email address (Class 2)
- **EV Code Signing Certificates** A unique organization name, business category, jurisdiction of incorporation of registration, registration number and physical address (Class 3).
- **SSL Certificates (Non EV types)** The minimum of a Domain Name (Class 1) within the Common Name attribute as approved as unique by ICANN coupled with an organization's name and state and/or locality. (Class 2)
- **SSL Certificates (EV)** The minimum of a Domain Name within the Common Name attribute as approved as unique by ICANN coupled with an organization's name, business category, jurisdiction of incorporation of registration, registration number and physical address (Class 3).
- **Timestamping Certificates** A unique organization name and state and/or locality with an optional email address (Class 2).
- **NAESB Rudimentary** A unique email address only. (Class 1)
- **NAESB Basic and Medium** A unique email address coupled with an organization's name and state and/or locality plus either the name of an individual or a department associated with the organization. (Class 2).
- **AATL Certificates** A minimum Class 2 Medium Assurance Certificate coupled with either the Organization only or a name of an individual affiliated with the Organization either as an employee, agent, contractor, business partner, or customer.
- **AATL & CDS** For Subordinate CAs with the ability to issue SSL certificates, the Baseline Requirements for Subject naming are followed. For all other types, Subject naming follows Class 2 practice of coupling a meaningful CA name with an organization's name and state and/or locality.
- **Qualified Certificates** Name of an Individual coupled with their details or organization name and organization state and/or locality coupled with affiliated Individual Name (Qualified Certificate for Qualified Electronic Signature) or an organization name and identifier and address (Qualified Certificate for Electronic Seal) (Class 3)

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

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

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

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered either as a Certificate Signing Request (CSR) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

GlobalSign accepts other Issuing CAs wishing to enter its hierarchy through its Trusted Root program. Following an initial assessment and signing of an agreement with GlobalSign, the Issuing CA must also prove possession of the Private Key. CA chaining services do not mandate the physical appearance of the Subscriber representing the Issuing CA so long as an agreement between the Applicant organization (which has been authenticated) and GlobalSign has been executed.

For Qualified Certificates, Subscriber keys must be generated and stored within a recognized Qualified Signature Creation Device (QSCD). The QSCD certification status must be monitored and appropriate measures must be taken if the certification status of a QSCD changes.

3.2.2 Authentication of Organization Identity

GlobalSign maintains internal policies and procedures which are reviewed regularly in order to comply with the requirements of the various root programs that GlobalSign is a member of, as well as the Baseline Requirements, the EV Guidelines and EV Code Signing Guidelines. These policy and procedure documents are under the control of PACOM5 – Subscriber Validation (subordinate to the main Policy Authority in section 1.5.1) fulfilling the criteria of Principle 6 of the WebTrust 2.1. The method by which GlobalSign verifies the organization identity is generally consistent across all product types, however alternative methods, in line with accepted alternatives, may be used where authentication is not possible through the more commonly used QGIS method outlined below.

For all Certificates that include an organization identity, Applicants are required to provide the organization's name and registered or trading address. For all Certificates, the legal existence, legal name, assumed name (if applicable), legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and requested address of the organization are verified using one of the following:

- A government agency (QGIS) in the jurisdiction of the Applicant, or a superior governing governmental agency if the Applicant claims they are a government agency themselves;
- A third-party database that is periodically updated and has been evaluated by GlobalSign to determine that it is reasonably accurate and reliable;
- An attestation letter confirming that Subject Identity Information is correct written by an accountant, a lawyer, a government official, a judge, or other reliable third party customarily relied upon for such information; or
- A Qualified Governmental Tax Information Source

Except for Extended Validation (which does not allow this method for verification of the address), GlobalSign may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that has been determined by GlobalSign to be reasonably accurate and reliable.

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

3.2.2.1 Local Registration Authority Authentication

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

3.2.2.2 Role Based Certificate Authentication (DepartmentSign)

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

3.2.2.3 Qualified Certificates

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

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

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

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

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

Additionally, GlobalSign may verify the address by reference to:

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

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

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

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

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

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

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

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

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

For any PSD2 Specific Attributes, GlobalSign will validate attributes using information provided by the National Competent Authority, which includes but is not limited to national public registers, European Banking Authority registers and authenticated communication from the National Competent Authority.

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

3.2.3 Authentication of Individual identity

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

3.2.3.1 Class 1

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

3.2.3.2 Class 2

The Applicant is required to demonstrate control of certain identity attributes included in the request, such as his/her email address or domain name to which the Certificate relates if included in the Certificate Request. This encompasses OV certificates.

The Applicant may also be required to submit a legible copy of a valid government issued national identity document or photo ID (driver's license, military ID or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. GlobalSign verifies to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information such as Country and/or state and locality fields are correct.

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

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

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

- Receiving an attestation from an appropriate notary or Trusted Third Party that they have verified the individual identity based on a Governmentally Accepted Form of ID.
- In the case of individuals affiliated with an organization: obtaining an executed declaration of identity of the individual that includes at least one unique biometric identifier of the individual (such as a fingerprint or handwritten signature). In this executed declaration of identity, an authorized representative of the Organization mentioned in the certificate confirms having seen the individual, reviewed the individual's photo ID, and confirm that the individual's identity information in the certificate requests matches the information contained in the reviewed photo ID. GlobalSign confirms the document's authenticity directly with the authorized representative of the organization using contact information confirmed using a Qualified Independent Information Source or a Qualified Government Information Source or any other method in line with the EV Guidelines. GlobalSign confirms

the authorized representative's authority to represent the Organization in line with the EV Guidelines.
- In the case of individuals affiliated with an organization, GlobalSign may rely on attestations from the approved Local RA. Refer to 3.2.3.5 in case of a Class 2 Certificate requested through an EPKI or an MSSL profile.
- Receiving an attestation from a customer to validate the identities of its own end customers based on a verification of a Governmentally Accepted Form of ID, while the customer maintains a secure auditable trail of these verifications.
- Other verifications in line with the verification of individuals for Qualified Certificates.

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

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

3.2.3.3 Class 3

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

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

The Applicant is required to submit a legible copy of a valid government issued national identity document or photo ID (driver's license, military ID or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. GlobalSign or a trusted third party verifies to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information such as Country and/or state and locality fields are correct.

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

"Trusted Third Party" means an entity that offers identity verification services in conformance with relevant rules and regulations and is certified by a third party as compliant with such rules and regulations.

For PersonalSign 3 Pro, a face to face meeting is required to establish the individual's identity with an attestation from the notary or trusted third party that they have met the individual and have inspected their national photo ID document, and that the application details for the order are correct. The Applicant is also required to demonstrate control of any email address to be included in a Certificate.

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

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

3.2.3.4 Qualified Certificates

GlobalSign authenticates the Identity of Individual Subscribers according to the following methods:
- In-person identity verification
- Using electronic identification means
- Using Qualified Signatures
- Video-verification

3.2.3.4.1 In-person Verification

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

- Government Issued Photo ID
- Signed personal statement
- Two secondary documentary evidences.

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

Entities that can perform this verification:

- Certification Authority (CA)
- Registration Authority (RA)
- Public Official or Third Party Validator
- Local Registration Authority - Organization (For Qualified Certificates that assert the individual's affiliation with an Organization. Identification of its employees, contractors, agents).

3.2.3.4.2 Using Remote Electronic Identification Means

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

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

The physical presence of the natural person can be ensured by looking at the categories of authentication factors the electronic identification means utilises. GlobalSign accepts the following authentication factors as proof of physical presence:

- At least one inherent factor; OR
- Multifactor with at least one factor in each of the following categories:
    - Possession-based ('possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it).
    - Knowledge-based ('knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it).

Entities that can perform this verification:

- Certification Authority (CA)
- Registration Authority (RA).

3.2.3.4.3 Qualified Certificates

GlobalSign uses the Subscriber's valid qualified electronic signature on a personal statement to verify the Applicant's identity and additional attributes contained in the Certificate used to create the qualified electronic signature.

GlobalSign will do so if the following conditions are met:

- Regardless of the Issuing CA, if the Qualified Certificate used for creation of the Qualified Electronic Signature was issued as part of a notified electronic identification scheme with high assurance level; OR
- If the Qualified Certificate was issued by GlobalSign following in-person identification less than 825 days prior to issuance of the new Certificate.

Entities that can perform this verification:
- Certification Authority (CA)
- Registration Authority (RA).

3.2.3.4.4 Video Verification

GlobalSign may use video verification. Similar to in-person verification, the Subscriber will be required to provide of the following documents:
- Government Issued Photo ID
- (Electronically) signed personal statement
- Two secondary documentary evidences.

The likeness of the Individual is compared to the Photo ID, and the security features of the Photo ID are inspected. This method requires that the Subscriber has access to an internet-enabled device, a working webcam or other video-equipment and a working microphone and sound-system.

Entities that can perform this verification:
- Certification Authority (CA)
- Registration Authority (RA).

3.2.3.5 Local Registration Authority Authentication

For Pre-vetted Organization accounts including EPKI and MSSL accounts, which allow the concept of a Local Registration Authority, GlobalSign sets authenticated organizational details in the form of a profile. Certificates issued within these accounts are populated with data fields from the profile. Suitably authenticated account administrators acting in the capacity of a Local Registration Authority are contractually obligated to authenticate individuals affiliated with the organization.

3.2.3.6 North American Energy Standards Board (NAESB) Certificates

For NAESB Certificate Requests, authenticity of organization identity requests for Certificates in the name of an affiliated organization shall include the organization name, address, and documentation of the existence of the organization. GlobalSign or the RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization. End entities using certificates for WEQ-012 applications shall be obligated to register their legal business identification and secure an "Entity Code" that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that end entity. When issuing Certificates for use within the energy industry for other than WEQ-012 applications, ACAs must comply with the provisions of the NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models, except provisions in WEQ-012-1.9.1, WEQ-012-1.3.3, and WEQ-012-1.4.3, which require End Entity registration within the NAESB EIR.

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

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

Registration of Identity Proofing Requirements shall use the following mappings:

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

GlobalSign, or its designated RA in the case of EPKI, shall verify all of the identification information supplied by the Applicant in compliance with the authentication requirements defined by the Identity Proofing Process (IPP) Method described in section 2.2.2: Authentication of Subscribers of the "NAESB Accreditation Requirements for Authorized Certification Authorities."

3.2.4 Non-Verified Subscriber Information

GlobalSign validates all information to be included within the Subject DN of a Certificate except as stated otherwise in this section of the CPS. GlobalSign uses the Subject: organizationalUnitName or Subject: serialNumber (non-EV/Qualified Certificates) as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices. In the case of individuals, a unique identifier such as mobile number may be used in conjunction with the individual's legal name.

- For all Certificate types where GlobalSign can explicitly identify a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity GlobalSign verifies the information and omits any disclaimer notice.

- For all Certificate types where GlobalSign cannot explicitly verify the identity, e.g. a generic term such as "Marketing", GlobalSign omits any disclaimer that this item is classified as non-verified Subscriber information as described herein. For IntranetSSL SSL/TLS Certificates only, GlobalSign relies upon information provided by the Applicant to be included within the subjectAlternativeName, such as internal or non-public DNS names, hostnames and RFC 1918 IP addresses.

Specifically for SSL/TLS Certificates and code signing Certificates, GlobalSign maintains an enrollment process which ensures that Applicants cannot add self-reported information to the subject: organizationalUnitName.

GlobalSign through its EPKI service provides certificates used most commonly used for client authentication, document signing, and secure messaging for end users, roles and devices. Local Registration Authorities are contractually obligated to perform validation of device names and/or roles and/or names. The following Policy OID (1.3.6.1.4.1.4146.1.40.10) is added in the Certificate in order to indicate that data included within the Certificate's Subject: organizationalUnitName and/or the common name has been verified by a LRA.

3.2.5 Validation of Authority

PersonalSign1 Certificates	Verification that the Applicant has control over the email address to be listed within the Certificate through a challenge response mechanism.
PersonalSignDemo Certificates	Verification that the Applicant has control over the email address to be listed within the Certificate.
PersonalSign2 Certificates	Verification through a reliable means of communication with the individual Applicant together with verification that the Applicant has control over any email address included.
Noble Energy Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included
NAESB Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included (see Section 3.2.3.5.)

PersonalSign2 Pro	Verification through a reliable means of communication with the individual Applicant together with verification that the Applicant has control over the email address included if required. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
PersonalSign2 Department Certificates	Verification through a reliable means of communication with the individual Applicant together with verification that the Applicant has control over the email address if an email address is requested to be included in the Certificate. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
PersonalSign3 Certificates	Verification through a reliable means of communication with the organization that the Applicant represents the organization. Personal appearance is mandatory before a suitable Registration Authority to validate the personal credentials of the Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate.
Code Signing Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address that may be optionally listed within the Certificate.
EV Code Signing Certificates	Verifying the authority of the contract signer and Certificate approver in accordance with the EV Guidelines and EV Code Signing Guidelines.
DV/AlphaSSL Certificates	Validation of the ownership or control of the domain name is performed via one of the domain validation methods defined in Section 3.2.7.
OV SSL & ICPEdu Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has ownership or control of the domain name via the methods listed in section 3.2.7. For Certificates issued through an MSSL account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
EV SSL Certificates	Verifying the authority of the contract signer and Certificate approver in accordance with the EV Guidelines together with verification that the Applicant has ownership or control of the domain name via the methods listed in section 3.2.7. For Certificates issued through an MSSL account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
Timestamping Certificates	Verification through a reliable means of communication with the organization's Applicant.
AATL and CDS	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over the email address if an email address is requested to be included in the Certificate. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
Trusted Root	Verification through a reliable means of communication with the organization's Applicant and verification of all elements included within 'Name Constraints' which may include top level e-mail domain/sub domain names or domain names as detailed in section 3.2.7.
Qualified Website Authentication Certificates	Verifying the authority of the contract signer/Certificate approver and the authorised representative in accordance with the methods listed in section 3.2.2.3 together with verification that the Applicant has ownership or control of the domain name via the methods listed in section 3.2.7.

Qualified Certificate for Electronic Seal	Verifying the authority of the contract signer Certificate approver and the authorised representative in accordance with the methods listed in section 3.2.2.3.
Qualified Certificate for Electronic Signature	Verification of the authenticity of the individual Applicant's request with the methods listed in section 3.2.3.4.

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

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

3.2.6 Criteria for Interoperation

As per 2.1.

3.2.7 Authentication of Domain Names

3.2.7.1 Authentication of FQDNs

For all SSL/TLS Certificates, authentication of the Applicant's (or the Applicant's parent company's, subsidiary company's or Affiliate's, collectively referred to as "Applicants" for the purposes of this section) ownership or control of all requested Domain Name(s) is done using one of the following methods:

1. Having the Applicant demonstrate control over the requested FQDN by sending a Random Value to a Domain Contact via email and then receiving a confirming response utilizing the Random Value. (BR section 3.2.2.4.2); or
2. Having the Applicant demonstrate control over the requested FQDN by calling the Domain Contact's (the Registrant's) phone number and obtaining a response confirming the Applicant's request for validation of the FQDN (BR section 3.2.2.4.3); and this method will not be used after May 31, 2019; or
3. Having the Applicant demonstrate control over the requested FQDN by sending a Random Value to an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name and obtaining a response utilizing the Random Value (BR section 3.2.2.4.4); or
4. Having the Applicant demonstrate control over the requested FQDN by confirming the presence of a Random Value within a file under the "/well-known/pki-validation" directory on an Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (BR section 3.2.2.4.18); or
5. Having the Applicant demonstrate control over the requested FQDN by confirming the presence of a Random Value in a DNS TXT record on an Authorization Domain Name (BR section 3.2.2.4.7); or
6. Having the Applicant demonstrate control over the requested FQDN by sending a Random Value to an email address sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A) (BR section 3.2.2.4.13); or
7. Having the Applicant demonstrate control over the requested FQDN by sending a Random Value to a DNS TXT Record Email Contact via email and then receiving a confirming response utilizing the Random Value (BR section 3.2.2.4.14); or
8. Having the Applicant demonstrate control over the requested FQDN by calling the Domain Contact's (the Registrant's) phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. (BR section 3.2.2.4.15); or
9. Having the Applicant demonstrate control over the requested FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs, provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified, and the DNS TXT Record Phone Contact provides a confirming response for each ADN (BR section 3.2.2.4.16).

GlobalSign uses methods 1-11 above for validating Wildcard FQDNs.

3.2.7.2 Authentication of IP Addresses

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

1. Having the Applicant demonstrate control over the requested IP address by confirming the presence of a Random Value within a file under the "/well-known/pki-validation" directory that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (BR section 3.2.2.5.1)
2. Having the Applicant demonstrate control of the IP address by sending a Random Value to a IP Address Contact via email and then receiving a confirming response utilizing the Random Value (BR section 3.2.2.5.2); or,
3. Performing a reverse IP address lookup and then verifying control over the resulting Domain Name using one of the options in section 3.2.7.1 (BR section 3.2.2.5.3); or
4. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation the IP Address (BR section 3.2.2.5.5).

3.2.8 Authentication of Email addresses

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

1. Having the Applicant demonstrate control over the requested email address by sending a Random Value to the requested email address and then receiving a confirming response utilizing the Random Value; or
2. Having the Applicant demonstrate control over or right to use the FQDN using one of the Domain Validation processes listed in Section 3.2.7. Once verified, an Enterprise RA can issue Certificates containing accurate email addresses under that FQDN.

3.3 Identification and Authentication for Re-key Requests

GlobalSign supports re-key requests from Subscribers prior to the expiry of the Subscriber's existing Certificate. GlobalSign also supports re-issue requests during the lifetime of the Certificate. Re-issue is a form of re-key, the primary difference being that the re-keyed Certificate has a 'Not-After' date which equals the 'Not After' date of the certificate that is being re-issued. Within the GCC re-key is called renew.

3.3.1 Identification and Authentication for Routine Re-key

- **PersonalSign1 Certificates** Username and password required with re-verification every 9 years.
- **PersonalSign2 Certificates** Username and password required with re-verification every 9 years or client authentication with a current unexpired and unrevoked Certificate.
- **Noble Energy Certificates** Username and password required with re-verification every 9 years or client authentication with a current unexpired and unrevoked Certificate.
- **PersonalSign3 Certificates** Username and password required with re-verification every 6 years.
- **Code Signing Certificates** Username and password required with re-verification every 825 days.
- **EV Code Signing Certificates** Username and password required with re-verification as indicated by the EV Guidelines and/or EV Code Signing Guidelines.
- **DV SSL Certificates** Username and password required with re-verification every 825 days.
- **OV SSL & ICPEdu Certificates** Username and password required with re-verification every 825 days.
- **EV SSL Certificates** Username and password required with re-verification as indicated by the EV Guidelines.
- **Timestamping Certificates** Not supported.
- **CA for AATL Certificates** Username and password required with re-verification every 6 years.

- **PDF Signing for Adobe CDS** Not supported
- **Trusted Root** Not supported
- **AlphaSSL** Not supported
- **NAESB Certificates** Subscribers of Authorized Certification Authorities shall identify themselves for the purpose of reissuing as required in the table below: Note GlobalSign does not issue NAESB High Assurance certificates.

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

- **Qualified Certificate for Electronic Seals** Username and password required with re-verification every 13 months.
- **Qualified Certificate for Electronic Signature** Username and password required with re-verification every 13 months.
- **Qualified Web Authentication Certificates** Username and password required with re-verification verification every 13 months, unless otherwise indicated by the EV Guidelines.

3.3.2 Identification and Authentication for Reissuance after Revocation

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

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

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

GlobalSign will not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.4 Identification and Authentication for Re-key After Revocation

A routine re-key after revocation is not supported. Re-key after revocation of a Certificate requires the Subscriber to follow the initial validation process that was previously completed to allow the initial issuance of the Certificate.

3.4 Identification and Authentication for Revocation Request

All revocation requests are authenticated by GlobalSign. Revocation requests may be granted following a suitable challenge response such as, logging into an account with the username and password, proving possession of unique elements incorporated into the Certificate (e.g. Domain Name or email address), or authentication of specific information from within the account which is authenticated out of band.

- **PersonalSign1 Certificates** Username and password or out of band.
- **PersonalSign2 & Pro Certificates** Username and password or out of band.
- **Noble Energy** Username and password or out of band.
- **NAESB Certificates** Username and password or out of band.
- **PersonalSign3 Pro Certificates** Username and password or out of band.
- **Code Signing Certificates** Username and password or out of band.
- **EV Code Signing Certificates** As indicated by the EV Guidelines.
- **DV SSL Certificates** Username and password or out of band or proof of possession of domain control using OneClickSSL.

- **AlphaSSL Certificates** Out of band or proof of possession of domain control using OneClickSSL.
- **OV SSL & ICPEdu Certificates** Username and password or out of band.
- **EV SSL Certificates** Username and password or out of band.
- **Timestamping Certificates** Out of band process.
- **CA for AATL Certificates** Username and password or out of band.
- **PDF Signing for Adobe CDS** Username and password or out of band.
- **Trusted Root** Out of band process.
- **Qualified Certificates** Username and password or out of band

GlobalSign may also perform revocation on behalf of Subscribers in accordance with the CPS and/or Subscriber Agreement.

4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

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

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

Applications are accepted via one of four methods:

- **On-line** Via a web interface over an https session. An Applicant must submit an application via a secure ordering process according to a procedure maintained by GlobalSign. Most direct customers use this method, known as GCC. It requires users to maintain an account with a suitably strong username and password for ongoing maintenance of the lifecycle of the Certificate. The account may be classified as MSSL, EPKI, retail, partner or reseller.
- **API** Resellers, partners and large enterprises may submit an appropriately formatted Certificate Request via an approved API (Application Programming Interface) to GlobalSign with a suitably strong username and password. The source IP address of the Applicant may be required by GlobalSign if no other constraints are applicable. The account may be classified as API or SAPI (Simple API).
- **Manual** Applicants that wish to issue timestamping certificates or require a greater number of SubjectAlternativeName entries in a Certificate than the GCC system supports are required to submit applications both electronically in the form of an email and out of band such that the request can be sufficiently authenticated and verified.

4.1.2 Enrollment Process and Responsibilities

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

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

- Generating a suitable Key Pair using a suitably secure platform;

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

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

(1) Prior to March 1, 2018, GlobalSign obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 39 months prior to issuing the Certificate; and

(2) On or after March 1, 2018, GlobalSign obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

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

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

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

4.2.2 Approval or Rejection of Certificate Applications

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

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

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

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

For Extended Validation, Qualified and Code Signing Certificates, separation of duties requires two members of the validation team to approve the request. GlobalSign operates in many jurisdictions; however, it may choose to outsource a pre-vetting function to suitably trained and experienced external RA partners who have additional relevant language and local jurisdiction knowledge to be

able to process and/or translate documentation that is not in a language that GlobalSign itself can process internally.

GlobalSign does not issue publicly trusted SSL certificates to internal server name or reserved IP addresses.

4.2.3 Time to Process Certificate Applications

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

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

The following approximations are given for processing and issuance.

- **PersonalSign1 Certificates** Approximately 1 minute
- **PersonalSign2 Certificates** Approximately 24-48 business hours
- **PersonalSign2 Pro Certificates** Approximately 36-72 business hours
- **Noble Energy Certificates** Approximately 1 minute (LRA only)
- **NAESB Certificates** Approximately 24-48 business hours
- **PersonalSign3 Pro Certificates** Approximately 48-72 business hours
- **Code Signing Certificates** Approximately 24-48 business hours
- **EV Code Signing Certificates** Approximately 48-96 business hours
- **DV SSL Certificates** Approximately[5] 1-5 minutes
- **AlphaSSL Certificates** Approximately[5] 1-5 minutes
- **OV SSL & ICPEdu Certificates** Approximately 24-48 business hours
- **EV SSL Certificates** Approximately 48-96 business hours
- **Qualified Certificates** Approximately 48-96 business hours
- **Timestamping Certificates** Approximately 5-10 business days
- **AATL Certificates** Approximately 24-48 business hours
- **CDS Certificates** Approximately 24-48 business hours
- **Trusted Root** 6-12 weeks including testing and the appropriate schedule of an offline key ceremony

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate issuance by GlobalSign Root CA requires an authorized Trusted Role member from GlobalSign to issue a direct command for the Root CA to perform a certificate signing operation.

GlobalSign shall ensure it communicates with any RA accounts capable of causing Certificate issuance using multi-factor authentication. This includes RAs directly operated by GlobalSign or RAs contracted by GlobalSign. Enterprise or local RA capabilities do not directly communicate with the CA and therefore multi-factor authentication is optional. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorized modification or tampering.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

---

[5] *In cases where the Domain Name to be validated for a DV/Alpha SSL Certificate is deemed to be high risk, the process followed will be closer to the processing time for OV SSL.*

4.3.3 Notification to North American Energy Standards Board (NAESB) Subscribers by the CA of Issuance of Certificate

Upon successful completion of the Applicant identification and authentication process GlobalSign shall issue the requested Certificate, notify the Applicant, and make the Certificate available to the Applicant.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

GlobalSign shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies GlobalSign within seven (7) days from receipt, the Certificate is deemed accepted.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties. GlobalSign's Subscriber Agreement identifies the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate. Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

In the case of GlobalSign's digital signing service, and with the consent of the Subscriber, GlobalSign shall host, secure, and manage short-lived Certificates and corresponding Private Keys.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CPS GlobalSign provides the conditions under which Certificates may be relied upon by Relying Parties including the appropriate Certificate services available to verify Certificate validity such as CRL and/or OCSP. GlobalSign provides a Relying Party agreement to Subscribers, the content of which should be presented to the Relying Party 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

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate and the same Public Key, with the exception of NAESB Certificates, which must rely on re-keying but contains a new 'Not After' date.

GlobalSign supports renewal for the following products and services:

- **PersonalSign1 Certificates** Renewal supported via GCC
- **PersonalSign2 Certificates** Renewal supported via GCC
- **PersonalSign2 Pro Certificates** Renewal supported via GCC
- **Nobel Energy Certificates** Renewal supported via GCC
- **PersonalSign3 Pro Certificates** Renewal supported via GCC
- **Code Signing Certificates** Renewal supported via GCC
- **EV Code Signing Certificates** Renewal supported via GCC
- **DV SSL Certificates** Renewal supported via GCC
- **AlphaSSL Certificates** Renewal supported via GCC
- **OV SSL & ICPEdu Certificates** Renewal supported via GCC
- **EV SSL Certificates** Renewal supported via GCC
- **Timestamping Certificates** Renewal supported via manual processes
- **NAESB Certificates** Renewal supported via GCC
- **AATL and CDS Certificates** Renewal supported via GCC
- **Qualified Certificates** Renewal supported via GCC
- **Managed SSL (MSSL)** Functions are built into the product
- **Enterprise PKI (EPKI)** Functions are built into the product
- **Trusted Root** Renewal supported via manual processes

GlobalSign may renew a Certificate so long as:

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

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

4.6.2 Who May Request Renewal

GlobalSign may accept a renewal request, provided that the original Subscriber, through a suitable Certificate lifecycle account challenge response such as a Subscriber's GCC account, authorizes it. For IETF RFC definition of renewal a Certificate signing request is not mandatory, however GlobalSign uses the term renewal to support a second application for a Certificate which is technically a re-key, however, the same Public Key may be used.

4.6.3 Processing Certificate Renewal Requests

GlobalSign may request additional information before processing a renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Certificate re-key is the process in which a Subscriber can obtain a new Certificate to replace an old Certificate that:

- Contains the same information (identity, domains etc.) as the old Certificate,
- Has the same expiry date (notAfter date) as the old Certificate,
- Contains a different Public Key as the old Certificate.

If a Certificate is re-keyed prior to the 'Not After' date, and the new Certificate is given the same 'Not After' date as the old Certificate, this process is referred to as Certificate reissue.

GlobalSign supports re-key and reissue for the following products and services:

- **PersonalSign1 Certificates** Re-key and reissue supported via GCC
- **PersonalSign2 Certificates** Re-key and reissue supported via GCC
- **PersonalSign2 Pro Certificates** Re-key and reissue supported via GCC
- **Nobel Energy Certificates** Re-key and reissue supported via GCC
- **PersonalSign3 Pro Certificates** Re-key and reissue supported via GCC
- **Code Signing Certificates** Re-key and reissue supported via GCC
- **EV Code Signing Certificates** Re-key and reissue supported via GCC
- **DV SSL Certificates** Re-key and reissue supported via GCC
- **AlphaSSL Certificates** Re-key and reissue supported via GCC.
- **OV SSL & ICPEdu Certificates** Re-key and reissue supported via GCC
- **EV SSL Certificates** Re-key and reissue supported via GCC
- **Timestamping Certificates** Re-key and reissue supported via manual processes
- **NAESB Certificates** Re-key and reissue supported via GCC
- **AATL and CDS Certificates** Re-key and reissue supported via GCC
- **Qualified certificates** Re-key and reissue supported via GCC
- **Managed SSL (MSSL)** Functions are built into the product
- **Enterprise PKI (EPKI)** Functions are built into the product
- **Trusted Root** Re-key and Reissue supported via manual processes

GlobalSign may re-key a Certificate as long as:

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

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

4.7.2 Who May Request Certification of a New Public Key

GlobalSign may accept a re-key request provided that it is authorized by the original Subscriber, or an organization administrator who retains responsibility for the Private Key on behalf of a Subscriber through a suitable Certificate lifecycle account challenge response. A Certificate signing request is mandatory with any new Public Key to be certified.

4.7.3 Processing Certificate Re-Keying Requests

GlobalSign may request additional information before processing a re-key or reissue request and may re-validate the Subscriber subject to re-verification of any previously validated data. In the case of a reissuance, authentication through a suitable challenge response mechanism is acceptable.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

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

- GlobalSign treats modification the same as 'New' issuance.
- GlobalSign may modify Certificates that have either been previously renewed or previously re-keyed. The original Certificate may be revoked after modification is complete, however, the original Certificate cannot be further renewed, re-keyed or modified.

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a CRL. The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding a serial number to the CRL allows Relying Parties to establish that the lifecycle of a Certificate has ended. GlobalSign may remove serial numbers when revoked Certificates pass their expiration date to promote more efficient CRL file size management, except for Code Signing certificates (10 years after expiry). Prior to performing a revocation GlobalSign will verify the authenticity of the revocation request.

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

1. The Subscriber requests in writing (to GlobalSign which provided the Certificate) that they wish to revoke the Certificate;
2. The Subscriber notifies GlobalSign that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. GlobalSign obtains reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. GlobalSign receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use, and/or unexpected termination of a subscriber's or subject's agreement or business functions.
5. GlobalSign obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

6. In case of PSD2 Certificates, GlobalSign receives an authenticated revocation request (or authenticates a revocation request) that originated from the NCA which has authorized or registered the payment service provider, and which includes a valid reason for revocation. Valid reasons for revocation include when the authorization of the PSP has been revoked or any PSP role included in the Certificate has been revoked.

Revocation of a Subscriber's Certificate should be performed within twenty-four (24) hours and is performed within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, as specified in Sections 6.1.5 and 6.1.6;
2. GlobalSign obtains evidence that the Certificate was misused;
3. GlobalSign is made aware of any circumstance indicating that used of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
4. GlobalSign is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
5. GlobalSign receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
6. GlobalSign is made aware that the Certificate was not issued in accordance with the Baseline Requirements or GlobalSign's CP or CPS;
7. GlobalSign determines that any of the information appearing in the Certificate is not accurate or is misleading;
8. GlobalSign ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
9. GlobalSign's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless GlobalSign has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by GlobalSign's CP and/or CPS;
11. The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);
12. GlobalSign is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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 GCC 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 blacklist, or is operating from a prohibited destination under the laws of GlobalSign's jurisdiction of operation;
4. Overdue payment of applicable fees by the Subscriber;
5. Following the request for cancellation of a Certificate;
6. If a Certificate has been reissued, GlobalSign may revoke the previously issued Certificate;
7. Under certain licensing arrangements, GlobalSign may revoke Certificates following expiration or termination of the license agreement;

8. 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;
9. If Microsoft, in its sole discretion, identifies a Code Signing or EV Code Signing Certificate as either containing a deceptive name or as being used to promote malware or unwanted software, Microsoft will contact GlobalSign and request that it revoke the Certificate. GlobalSign will either revoke the Certificate within a commercially-reasonable timeframe or request an exception from Microsoft within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. If Microsoft does not grant the exception, GlobalSign will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days; or
10. If Microsoft, it its sole discretion, identifies an SSL Certificate is being used to promote malware or unwanted software, Microsoft will contact GlobalSign and request that it revoke the Certificate. GlobalSign will either revoke the Certificate within a commercially-reasonable timeframe or request an exception from Microsoft within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, GlobalSign will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days;
11. Death of a Subscriber.

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

1. The Subordinate CA requests in writing to the GlobalSign entity which provided the Subordinate CA Certificate, or the authority detailed in Section 1.5.2 of this CPS, that GlobalSign revoke the Certificate;
2. The Subscriber notifies the 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 Baseline Requirements 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 Baseline Requirements or applicable CP or CPS;
6. GlobalSign determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's CP and/or CPS;
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

For any Trusted Root CA, GlobalSign may revoke the Issuing CA if the Trusted Root CA no longer meets the contractual terms and conditions of the agreement between the two parties.

4.9.2 Who Can Request Revocation

GlobalSign and RAs will accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the Certificate. Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify GlobalSign of a suspected reasonable cause to revoke the Certificate. Additionally for PSD2 Certificates, revocation request can originate from the NCA which has authorized or registered the payment service provider.
GlobalSign may also at its own discretion revoke Certificates including Certificates that are issued to other cross signed CAs.

4.9.3 Procedure for Revocation Request

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

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

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

4.9.4 Revocation Request Grace Period

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

For all other Certificates, the revocation request grace period is the time available for a Subscriber to take any necessary actions themselves to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate. Subscribers are given 48 hours to take appropriate actions, otherwise GlobalSign may revoke the Certificate. A risk analysis shall be completed and recorded for any revocations that cannot be processed by either party for any reason.

4.9.5 Time Within Which CA Must Process the Revocation Request

All revocation requests for end entity Certificates, both those generated automatically via user accounts and those initiated by GlobalSign itself, must be processed within a maximum of 24 hours of receipt.

GlobalSign, through its Trusted Root program, processes revocation requests within 24 hours of a confirmation of Compromise and an ARL is published within 12 hours of its creation.

GlobalSign maintains 24 x 7 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. GlobalSign will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

GlobalSign decides whether revocation or other action is warranted based on at least the following criteria:

- The nature of the alleged problem;
- The number of reports received about a particular Certificate or Subscriber;

- The entity making the complaint; and
- Relevant legislations.

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 ensure the Certificate is valid. Relying Parties will need to consult the CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). GlobalSign will include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process such as:

- http://crl.globalsign.net
- http://crl.globalsign.com/
- http://crl.globalsign.com/gs/
- http://ocsp.globalsign.com
- http://ocsp2.globalsign.com
- http://crl2.alphassl.com/gs/
- http://crl.alphassl.com/

PDF signing Certificates also require Relying Parties to check the status of the Adobe Root CRL. This CRL is outside the scope of this CPS but is located at http://crl.adobe.com/cds.crl.

4.9.7 CRL Issuance Frequency

If an End Entity certificate contains a CDP (CRL Distribution Point) then that CRL is updated at least every 7 days (every 24 hours for Qualified Certificates' CRLs) and value of the nextUpdate field is not more than 10 days beyond the value of the thisUpdate field.

If a CA certificate contains a CDP, then that CRL is updated at least once every 12 months and within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than 12 months beyond the value of the thisUpdate field.

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

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 supports OCSP responses in addition to CRLs. Response times are generally no longer than 10 seconds under normal network operating conditions.

GlobalSign OCSP responses conforms to RFC6960 and/or RFC5019. 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. OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation, information otherwise all warranties become void.

For the status of Subscriber Certificates:

- GlobalSign updates information provided via an OCSP at least every four days. OCSP responses from this service will not exceed an expiration time of seven days.

For the status of Subordinate CA Certificates:

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

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

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

GlobalSign requires OCSP requests to contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

4.9.11 Other Forms of Revocation Advertisements Available

4.9.12 Special Requirements Related to Key Compromise

GlobalSign and any of its Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where GlobalSign at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, GlobalSign shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRLs within 30 minutes of creation and ARLs within 12 hours.

4.9.13 Circumstances for Suspension

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

Certificate suspension will not be supported for Qualified Certificates.

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

4.10.1 Operational Characteristics

GlobalSign provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both in the certificates. For Code Signing Certificates and Qualified Certificates that include a cRLDistributionPoints extension, GlobalSign does not remove revocation entries on CRL or OCSP until 10 years after the Expiry Date of the revoked Certificate. For other Certificate types, GlobalSign does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

GlobalSign sends email notification to subscribers in the month (typically 30 days and 7 days) before expiry informing subscribers about upcoming expiration of their certificates.

4.10.2 Service Availability

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

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

4.10.3 Operational Features

No stipulation

4.11 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire. For Trusted Root, contracts between GlobalSign and the Trusted Root Subscriber must be maintained throughout the life of the Certificate, unless Certificate revocation is used by GlobalSign as a method to terminate the contract.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed. GlobalSign does not offer key escrow services to Subscribers.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

GlobalSign's Certificate Management Process MUST include:

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

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 develops, implements, 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 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

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

5.1.1 Site Location and Construction

GlobalSign's CAs are located within a secure data center. The data center is a purpose-built facility made of concrete and steel construction.

5.1.2 Physical Access

GlobalSign's CAs are operated within a secure data center that provides premise security with biometric scanners and card access systems. A 24x7 Closed Circuit TV (CCTV) monitoring system as well as digital recording is provided. Qualified 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 a secure data center that is equipped with redundant power and cooling system. UPS and failover to power generator are in place in the unlikely event of power outage.

5.1.4 Water Exposures

GlobalSign's CAs are protected against water. It is 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 a secure data center that is equipped with a fire detection and suppression system.

5.1.6 Media Storage

Storage of backup media is off-site, 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 destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

GlobalSign performs regular off-site backup of critical data. The backed-up data is stored at a physically secured off-site location.

5.2 Procedural Controls

5.2.1 Trusted Roles

GlobalSign ensures that all operators and administrators including Vetting Agents are acting in the capacity of a trusted role. Trusted roles are such that no conflict of interest is possible, and the roles are distributed such that no single person can circumvent the security of the CA system.

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

Trusted roles include but are not limited to the following:

- **Developer:** Responsible for development of CA systems.
- **Security Officer/Head of Information Security:** Overall responsibility for administering the implementation of the CA's security practices;
- **Vetting Agents:** Responsible for validating the authenticity and integrity of data to be included within Certificates via a suitable RA system and approve the generation/revocation/suspension of Certificates;
- **Infra System Engineer:** Authorized to install, configure and maintain the CA systems used for Certificate lifecycle management;
- **Infra Operator:** Responsible for operating the CA systems on a day to day basis. Authorized to perform system backup / recovery, viewing / maintenance of CA system archives and audit logs;
- **Auditor:** Authorized to view archives and audit logs of the CA Trustworthy Systems;
- **CA activation data holder:** Authorized person that holds CA activation data that is necessary for CA hardware security module operation.

5.2.2 Number of Persons Required per Task

The 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.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, GlobalSign performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 Roles Requiring Separation of Duties

GlobalSign enforces role separation either by the CA equipment or procedurally or by both means.

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 (e.g., key component custodians);
- Those performing CA systems development.

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.

GlobalSign employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function.

GlobalSign personnel fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. GlobalSign personnel (both temporary and permanent) have job descriptions 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 analysed, provided such checks are permitted by the jurisdiction in which the person will be employed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation 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 the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and the Baseline Requirements.

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

GlobalSign documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

GlobalSign requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements.

5.3.4 Retraining Frequency and Requirements

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

Individuals responsible for trusted roles are aware of changes in the GlobalSign or RA operations, as applicable. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented.

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

5.3.5 Job Rotation Frequency and Sequence

GlobalSign ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Contractor personnel employed for GlobalSign operations are subject to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

GlobalSign makes available to its personnel this CPS, any corresponding CP and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

GlobalSign ensures all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

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

GlobalSign records details of the 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 as proof of the CA's compliance with associated CA audit scheme stipulated in introduction.

GlobalSign records at least the following events:
CA key life cycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device life cycle management events; and
- CA system equipment configuration.

CA and Subscriber Certificate life cycle management events, including:

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

Security events, including:

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

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

GlobalSign retains any audit logs generated for at least ten years. GlobalSign makes these audit logs available to Qualified Auditor upon request.

5.4.4 Protection of Audit Log

The 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 trusted 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 realisation.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

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 the case of a problem occurring during the process of the audit collection GlobalSign determines whether to suspend GlobalSign operations until the problem is resolved, duly informing the GlobalSign impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

GlobalSign performs annual risk assessments that:

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

GlobalSign also performs regular vulnerability assessment and penetration testing covering all GlobalSign assets related to Certificate issuance, products and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the Certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

GlobalSign and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system.

5.5.2 Retention Period for Archive

GlobalSign retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least 10 years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

The archives are created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive

protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

Archive backups are made which are either of the online GlobalSign system or the offline system. Online backups are duplicated weekly and each backup is stored in a location which is different from the original online system. One backup is stored in a fire rated media safe. An offline backup is taken at the end of any key ceremony (with the exception of any encrypted material which is store separately in line with key ceremony procedures) and stored in an off-site location within 30 days of the ceremony.

5.5.5 Requirements for Timestamping of Records

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

5.5.6 Archive Collection System (Internal or External)

The archive collection system complies with the security requirements in Section 5.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of GlobalSign archive information is checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorised GlobalSign equipment, trusted role and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are coordinated by operators in trusted roles (internal auditor, the manager in charge of the process and the security officer).

5.6 Key Changeover

GlobalSign may periodically change over 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 are maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

GlobalSign has an Incident Response Plan and a Disaster Recovery Plan. 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.

GlobalSign does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity plan and security plans to the GlobalSign's CA auditors upon request.

GlobalSign annually tests, reviews, and updates these procedures. The business continuity plan includes:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;

10. GlobalSign's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time;
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. 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.

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

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

5.7.3 Entity Private Key Compromise Procedures

In the event a GlobalSign Private Key is Compromised, lost, destroyed or suspected to be Compromised:

- GlobalSign, after investigation of the problem, shall decide if the GlobalSign Certificate should be revoked. If so, then:
    - All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and
    - A new GlobalSign Key Pair shall be generated, or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability.

5.8 CA or RA Termination

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

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

5.8.1 Successor Issuing Certification Authority

To the extent that it is practical and reasonable, the successor Issuing CA should assume the same rights, obligations and duties as the terminating Issuing CA. The successor Issuing CA should issue new Keys and Digital Certificates to all subordinate service providers and Users whose Keys and Digital Certificates were revoked by the terminating Issuing CA due to its termination, subject to the

individual service provider or User making an application for a new Digital Certificate, and satisfying the initial registration and Identification and Authentication requirements, including the execution of a new service provider or Certificate Holder Agreement.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

For Root CA Key Pairs, GlobalSign performs following controls;

1. prepares and follows a Key Generation Script,
2. has a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. has a Qualified Auditor issue a report opining that GlobalSign 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.

In other CA Key Pairs, GlobalSign performs following controls:

1. Generates the keys in a physically secured environment as described in Section 5.1 and 5.2.2. of Certificate Policy and/or Certification Practice Statement;
2. Generates the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. Generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. Log its CA key generation activities; and
5. 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 Subscriber Key Pair Generation

For Subscriber keys generated by GlobalSign, Key generation is performed in a secure cryptographic device that meets FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

GlobalSign also rejects a certificate request if it has a known weak Private Key.

For Qualified Certificates, Subscriber keys are generated and stored within a recognized Qualified Signature Creation Device (QSCD). The QSCD certification status is monitored and appropriate measures will be taken if the certification status of a QSCD changes.

6.1.2 Private Key Delivery to Subscriber

GlobalSign CAs that create Private Keys on behalf of Subscribers do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. For SSL/TLS Certificates, this is achieved through the use of PCKS#12 (.pfx) files containing Private Keys and Certificates encrypted by at least sixteen (16) character password. At least eight (8) characters are system generated and provided to the Subscriber during the enrolment process and the Subscriber specifies at least eight (8) characters. For SMIME certificates, this is again achieved through the use of PCKS#12 (.pfx) files containing Private Keys and Certificates encrypted by a minimum twelve (12) alpha-numeric character Subscriber-selected password.

GlobalSign does not generate Private Keys for publicly trusted SSL certificates.

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

6.1.3 Public Key Delivery to Certificate GlobalSign

GlobalSign only accepts Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2.1 of this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

GlobalSign follows NIST Special Publication 800-133 (2012) - Recommendation for Cryptographic Key Generation - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Issuing CAs and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root program, outside of the direct control of GlobalSign are contractually obligated to use the same best practices.

GlobalSign selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the SSL Baseline Requirements and EV Guidelines.

Certificates must meet the following requirements for algorithm type and key size.

Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA- 512
Minimum RSA modulus size (bits)	2048[6]	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

Subordinate Certificates

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1[7], SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

Subscriber Certificates

Digest algorithm	SHA-1[8], SHA-256, SHA-384 or SHA- 512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
RSASSA-PSS[9]	

[6] *A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.*

[7] *SHA-1 Is used for IntranetSSL Subscriber and subordinate CA Certificates, but they are not chained to publicly trusted roots.*

[8] *SHA-1 MAY be used with RSA keys for PersonalSign Certificates and Code Signing Certificates in accordance with the criteria defined in Section 7.1.3.*

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

6.1.6 Public Key Parameters Generation and Quality Checking

GlobalSign generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys are tested for and rejected at the point of submission. GlobalSign references the Baseline Requirements Section 6.1.6 on quality checking.

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

GlobalSign sets key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (see Section 7.1).

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

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

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 above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. GlobalSign encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

GlobalSign ensures that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection. CAs that require Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection. A suitable mechanism used by GlobalSign is the limitation to a suitable CSP (Cryptographic Service Provider) tied to a known FIPS compliant hardware platform as part of the enrollment process.

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

GlobalSign activates Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code). The Root Certificate Private Key is always protected through 3 of X.

6.2.3 Private Key Escrow

GlobalSign does not escrow Private Keys for any reason.

6.2.4 Private Key Backup

If required for business continuity GlobalSign backs up Root and Subordinate Private Keys under the same multi-person control as the original Private Key. GlobalSign does not backup Subscriber Private Keys.

6.2.5 Private Key Archival

With the exception of GlobalSign's digital signing service, GlobalSign does not archive Subscriber Private Keys and ensures that any temporary location where a Private Key may have existed in any memory location during the generation process is purged.

6.2.6 Private Key Transfer into or from a Cryptographic Module

GlobalSign 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 Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

GlobalSign is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

GlobalSign Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that GlobalSign destroys all associated CA secret activation data in the HSM in such a manner that no information can be used to deduce any part of the Private Key.

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

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

GlobalSign archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

GlobalSign Certificates and renewed Certificates have a maximum Validity Period of:

Type	Private Key Usage	Max Validity Period
Root Certificates[10]	25 years	40 years
TPM Root Certificates	30 years	40 years
Publicly Trusted Sub-CAs/Issuer CAs	No stipulation	17 years
Trusted Root	No stipulation	10 years
PersonalSign Certificates	No stipulation	39 months
Noble Energy Certificates	No stipulation	5 years
Code Signing Certificates	No stipulation	39 months
EV Code Signing Certificates	No stipulation	39 months
AATL End Entity Certificates	No stipulation	39 months
Qualified Certificate for Electronic Seals and Qualified Certificate for Electronic Signatures	No stipulation	39 months
DV SSL Certificates	No stipulation	825 days
AlphaSSL Certificates	No stipulation	825 days
OV SSL & ICPEdu Certificates	No stipulation	825 days
Intranet SSL	No stipulation	5 years

[10] *2048-bit keys generated prior to 2003 using RSA may be used for 25 years due to limited usage due to key size restrictions within hardware, root stores and operating systems.*

EV SSL Certificates	No stipulation	27 months
Timestamping Certificates	15 months	11 years
PDF Signing for Adobe CDS Certificates	No stipulation	39 months
NAESB Certificates	2 years	2 years
Qualified Website Authentication Certificates	No stipulation	27 months

Key Pair usage period can have up to the same Validity Period as Certificate Validity Period.

Certificates signed by a specific CA must expire before the end of that Key Pair's operational period.

GlobalSign complies with the Baseline Requirements with respect to the maximum Validity Period. In the event that a Subscriber's Certificate has a reduced validity period, subsequent reissues may be used to regain that lost validity period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of GlobalSign activation data used to activate GlobalSign Private Keys are made during a key ceremony (Refer to Section 6.1.1). Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. It is then delivered to a holder of a share of the key 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

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

6.4.3 Other Aspects of Activation Data

GlobalSign 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 computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The GlobalSign PKI components must include the following functions:

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

For accounts capable of directly causing certificate issuance, GlobalSign enforces multifactor authentication.

6.5.2 Computer Security Rating

A version of GlobalSign's core software is Common Criteria EAL4+ certified.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for GlobalSign are as follows:

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

6.6.2 Security Management Controls

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

6.6.3 Lifecycle Security Controls

GlobalSign maintains a maintenance scheme to ensure the level of trust of software and hardware that are evaluated and certified.

6.7 Network Security Controls

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

6.8 Timestamping

All GlobalSign components are regularly synchronized with a reliable time service. GlobalSign uses one GPS source, one DCF77 source, and three non-authenticated NTP source clocks to establish the correct time for:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

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

6.8.1 PDF Signing Timestamping Services

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

Timestamping services may be provided by GlobalSign or by a GlobalSign outsource agent. In the event that a timestamping service is managed by an outsource agent, then GlobalSign will issue a timestamping Certificate in compliance with this CPS.

6.8.2 Code Signing and EV Code Signing Timestamping Services

All Digital Signatures created by Code Signing and Extended Validation Code Signing Certificates have the ability to include a trusted timestamp issued from an RFC 3161 compliant Time Stamp Authority (TSA) server chained to a GlobalSign Root Certificate. The TSA certificate shall be located in a FIPS 140-2 level 2 or higher HSM. Timestamping services may be provided by GlobalSign or by a GlobalSign outsource agent. In the event that a timestamping service is managed by an outsource agent, then GlobalSign will issue a timestamping Certificate in compliance to this CPS.

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

GlobalSign issues Certificates in compliance with RFC 5280 and applicable best practice including compliance to the current CA/B Forum Baseline Requirements section 7.1.2.1 through 7.1.2.5. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

GlobalSign issues Certificates with algorithms indicated by the following OIDs:

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
ECDSAWithSHA1	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) 1 }
ECDSAWithSHA224	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2 }
ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ECDSAWithSHA512	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }
RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)}

7.1.4 Name Forms

GlobalSign issues Certificates with name forms compliant to RFC 5280 and section 7.1.4 of CA/B Forum Baseline Requirements for SSL, EV Code Signing certificates that chain up to Publicly Trusted Root.

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.5 Name Constraints

GlobalSign may issue Subordinate CA Certificates with name constraints where necessary and mark as critical where necessary as part of the Trusted Root program. When name constraints are NOT set on a Subordinate CA, such CA must be subject for full audit specified in section 8.0 of this document.

GlobalSign name constrains using the following methods:

- If the certificate includes the id-kp-serverAuth extended key usage, then the certificate MUST be name constrained with constraints on dNSName, iPAddress and DirectoryName as described in section 7.1.5 of version 1.3 or later of the Baseline Requirements.
- If the certificate includes the id-kp-emailProtection extended key usage, it MUST include the name constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

- GlobalSign MAY also include name constraints on certificates with the id-kp-emailProtection extended key usage with constraints on dNSName, iPAddress and DirectoryName as described in section 7.1.5 of version 1.3 or later of the Baseline Requirements

7.1.6 Certificate Policy Object Identifier

GlobalSign follows Section 7.1.6 of CA/B Forum Baseline Requirements.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.1.10 Serial Numbers

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

7.1.11 Special Provisions for Qualified Certificates

7.1.11.1 Qualified Signatures

Qualified Signature certificates will contain following qualified statements

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
- id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
  esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign)

7.1.11.2 Qualified Seals

Qualified Seal certificates will contain following qualified statements:

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
- id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-eseal)

7.1.11.3 Qualified Web Authentication Certificates

Qualified Web Authentication Certificates will contain the following qualified statements:

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }

- id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE { qcType OBJECT IDENTIFIER {{id-etsi-qct-web}}}CRL Profile

7.1.12 Version Number(s)

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

- **Issuer** The Subject DN of the issuing CA
- **Effective date** Date and Time
- **Next update** Date and Time
- **Signature Algorithm** sha1RSA, sha256RSA etc. (Depending upon product)
- **Signature Hash Algorithm** sha1, sha256 etc. (Depending upon product)
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

7.1.13 CRL and CRL Entry Extensions

CRLs have the following extensions:

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

7.2 OCSP Profile

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

7.2.1 Version Number(s)

GlobalSign issues Version 1 OCSP responses with following fields:

- Responder ID SHA-1 Hash of responder's Public Key
- Produced Time The time at which this response was signed
- Certificate Status Certificate status referenced (good/revoked/unknown)
- ThisUpdate/NextUpdate Recommended validity interval for the response
- Signature Algorithm SHA1 RSA, SHA256 RSA etc. (depending upon product)
- Signature Signature value generated by the responder
- Certificates The OCSP Responder's Certificate

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

7.2.2 OCSP Extensions

If OCSP request has a nonce field, then the corresponding response also has the same nonce value in the response.

8.0 Compliance Audit and Other Assessments

The procedures within this CPS encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which GlobalSign operates. Trusted Root CAs that are not constrained by dNSNameConstraints are audited for compliance to one or more of the following standards:

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

8.1 Frequency and Circumstances of Assessment

GlobalSign maintains its compliance with the AICPA/eIDAS standards identified above via a Qualified Auditor on an annual (AICPA), bi-annual (eIDAS) and contiguous basis. The audit covers all of GlobalSign's activities.

8.2 Identity/Qualifications of Assessor

The audit of GlobalSign is performed by Ernst & Young as a "Qualified Auditor" that possesses the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an internal government auditing agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million ($1,000,000) 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 and in particular against the requirements defined in the eIDAS Regulation (EU) No 910/2014.

8.3 Assessor's Relationship to Assessed Entity

GlobalSign has selected an auditor/assessor who is completely independent from GlobalSign.

8.4 Topics Covered by Assessment

The audit meets the requirements of the audit schemes highlighted in Section 8.0 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to GlobalSign in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communications of Results

Results of the audit are reported to the Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan. The results could also be made available to any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement. Copies of GlobalSign's WebTrust for CAs audit reports can be found at: https://www.globalsign.com/en/repository/

8.7 Self-Audit

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

9.0 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 (re-key during the lifetime of the Certificate). 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

GlobalSign offers a refund to Subscribers in accordance with the refund policy published on GlobalSign's web site https://www.globalsign.com/repository. Subscribers who choose to invoke the refund policy should have all issued Certificates revoked.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

GlobalSign nv-sa maintains commercial general liability insurance with policy limits of at least two million US dollars ($2,000,000) in coverage and Errors and Omissions / Professional Liability insurance with a policy limit of at least five million US dollars ($5,000,000) in coverage. GlobalSign's insurance policies include coverage for (1) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (2) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, patent, and trademark infringement), invasion of privacy, and advertising injury. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End Entities

GlobalSign offers a Warranty Policy to Subscribers published on GlobalSign's web site at https://www.globalsign.com/repository.

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 staff including Vetting Agents and administrators:

- Personal Information as detailed in Section 9.4;
- Audit logs from CA and RA systems;
- Activation data used to active 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

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

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 web site at https://www.globalsign.com/repository.

9.4.2 Information Treated as Private

GlobalSign treats all information received from Applicants that will not ordinarily be placed into a Certificate as private. This applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected. GlobalSign periodically trains all RA and vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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. Any backup of private information must be encrypted when transferred to suitable backup media. The Privacy Policy is published on GlobalSign's web site at https://www.globalsign.com/repository.

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.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

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 CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. All parties including GlobalSign, any RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been Compromised they will immediately notify the appropriate RA.

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:

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, GlobalSign (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, GlobalSign (i) operated a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, GlobalSign (i) operated a procedure for verifying all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) was true and accurate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, GlobalSign (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) operated a procedure to verify the identity of the Applicant and that for Code Signing Certificates this procedure at least meets the requirements of section 11 of the Baseline Requirements for Code Signing ; (ii) followed the procedure when issuing and managing the Certificate; and (iii) accurately described the procedure in GlobalSign's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if GlobalSign and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, Baseline Requirements for Code Signing (if applicable) or, if GlobalSign and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);
- **Status:** That GlobalSign maintains a 24 x 7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates and that for Code Signing Certificates will maintain the Repository for the period required by the Baseline Requirements for Code Signing;
- **Revocation:** That GlobalSign will revoke the Certificate for any of the reasons specified in the Baseline Requirements, Baseline Requirements for Code Signing, EV Guidelines and/or EV Code Signing Guidelines (as applicable) (see Section 4.9.1); and
- **Compliance**: That, for Code Signing Certificates, GlobalSign has complied with the Baseline Requirements for Code Signing and the applicable Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate and operating its PKI.
- **Key Protection:** That, for Code Signing Certificates, GlobalSign represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates.

In addition, GlobalSign represents and warrants to Certificate Beneficiaries for NAESB Certificates that, 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:

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

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

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

9.6.2 RA Representations and Warranties

RAs warrant that:

- Issuance processes are in compliance with this CPS 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

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 review and verify the Certificate contents for accuracy;
- **Use of Certificate:** Subscriber shall install an SSL Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- **Reporting and Revocation:** Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- **Termination of Use of Certificate:** Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate; and
- **Responsiveness:** Subscriber shall respond to GlobalSign's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours.

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 GlobalSign discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.3.1 North American Energy Standards Board (NAESB) Subscribers

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

Registered end entities and the user community they represent shall be required to meet to all end entity obligations in the NAESB WEQ PKI Standards.

Each Subscriber organization acknowledges their understanding of the following obligations of the NAESB WEQ PKI Standards through GlobalSign as follows:

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

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

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

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

B. End entity has evaluated each of its selected Certification Authority's Certification Practice Statement in light of those industry standards as identified by the Certification Authority.

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

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

- Protect their Private Keys from access by other parties.
- When applicable, identify, through the NAESB EIR, the specific entity they have selected GlobalSign to use as their Authorized Certification Authority.
- Execute all agreements and contracts with GlobalSign as required by GlobalSign's Certification Practice Statement necessary for GlobalSign to issue Certificates to the end entity for use in securing electronic communications.
- Comply with all obligations required and stipulated by GlobalSign in this CPS, e.g., Certificate application procedures, Applicant identity proofing/verification, and Certificate management practices.
- Confirm that it has a PKI Certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to:
    - Certificate Private Key security and handling policy(ies)
    - Certificate revocation policy(ies)
- Identify the type of Subscriber (I.e., individual, role, device or application) and provide complete and accurate information for each Certificate Request.

9.6.4 Relying Party Representations and Warranties

A party relying on an Issuing CA's Certificate warrants to:

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

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

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

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

9.6.4.1 North American Energy Standards Board (NAESB) Relying Parties

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

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

9.6.5 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 BASELINE REQUIREMENTS AND THIS CPS, GLOBALSIGN SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE, GLOBALSIGN'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS ($1,000) PER CERTIFICATE; PROVIDED HOWEVER THAT THE LIMITATION SHALL BE TWO THOUSAND DOLLARS ($2,000) PER CERTIFICATE FOR AN EV CERTIFICATE OR AN EV CODE SIGNING CERTIFICATE.

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

IN NO EVENT SHALL GLOBALSIGN SHALL 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 CPS.

9.9 Indemnities

9.9.1 Indemnification by GlobalSign

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

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify GlobalSign, its partners, and 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 CPS, 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 CPS, 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 CPS 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 CPS termination via the appropriate Repository.

9.11 Individual Notices and Communications with Participants

GlobalSign accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from GlobalSign the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the sender. Individuals communications made to GlobalSign must be addressed to: legal@globalsign.com or by post to GlobalSign in the address provided in Section 1.5.2.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate 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 CPS as well as any appropriate period by when the revised CPS is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

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

Upon receipt of a dispute notice, GlobalSign convenes a dispute committee that advises GlobalSign management on how to proceed with the dispute. The dispute committee convenes within twenty (20) business days from receipt of a dispute notice. The dispute committee is composed of a counsel, a data protection officer, a member of GlobalSign operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the dispute committee proposes a settlement to the GlobalSign executive management. The GlobalSign executive management may subsequently communicate the proposed settlement to the complaining party.

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to 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 CPS is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CPS, 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 CPS 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 CPS 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 CPS cannot assign their rights or obligations without the prior written consent of GlobalSign.

9.16.3 Severability

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

Each provision of this CPS 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 CPS does not waive GlobalSign's right to enforce the same provisions later or right to enforce any other provisions of this CPS. 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

Third party Issuing CAs that want to subscribe to the Trusted Root CA chaining service of GlobalSign must adhere to this CPS and all of its conditions. This adherence is implemented and verified through a number of legal and procedural controls and is verified through annual audits. Controls include, but are not limited to:

- Execution of a CA chaining agreement between the Trusted Root Subscriber and GlobalSign;
- Submission and publication of a CPS reviewed and acceptance by GlobalSign and/or GlobalSign auditors; and
- Submission of PKI infrastructure review by Trusted Root Subscriber and acceptance by GlobalSign and/or GlobalSign auditors.

9.17.1 CA Chaining Agreement

The CA chaining Agreement includes the following terms and conditions:

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

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

9.17.2 PKI Infrastructure review

Execution of Trusted Root Subscriber Agreement is subject to review and acceptance by GlobalSign and/or GlobalSign auditors of Subscriber PKI infrastructure review.

This review documents the Subscriber CA hierarchy and its security measures taken. It includes, but is not limited to, the following subjects:

- Logical security measures implemented – including personnel matters and separation of duty and dual control;
- Physical security measures implemented;
- Network security measures implemented;
- CA hierarchy implemented; and
- HSM type and serial numbers.

9.17.3 Subscriber CA implementation

GlobalSign requires a mandatory test signing of a Subscriber CA with a GlobalSign test CA. GlobalSign test CA duplicates the GlobalSign Root CA but it is identified as for testing purposes

(CAT versus CA) and is not distributed to third party applications. Only after successful test signing is the Subscriber CA signed by GlobalSign Root CA.

9.17.4 Ongoing requirements and audits

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