GlobalSign

Certification Practice Statement

Certificates issued under Singapore Law

Date: March 29, 2024

Version: v1.0

Table of Contents

Document History

Version	Release Date	Status & Description
v1.0	March 29, 2024	Initial release

Acknowledgments

1.0 Introduction

1.1 Overview

This Certification Practice Statement ("CPS" or “Singapore CPS”) outlines the certification practices for GMO GlobalSign Pte. Ltd, entity identification number 201003472C, and affiliated entities ("GlobalSign") Public Key Infrastructure for Certificates issued in accordance with the Singapore Electronic Transactions Act 2010 (“ETA”) and Electronic Transactions (Certification Authority) Regulations 2010 ("ETR").

CERTIFICATES ISSUED UNDER THIS CPS, WITH A NATURAL PERSON SUBJECT, ARE CONSIDERED TRUSTWORTHY WITHIN THE MEANING OF REGULATION 3(B)(I) OF THE THIRD SCHEDULE TO THE ETA. WHEN TRUSTWORTHY CERTIFICATES ARE USED FOR DIGITAL SIGNATURE, THEY ARE TREATED AS SECURE ELECTRONIC SIGNATURES WITHIN THE MEANING OF THE ETA. SECURE ELECTRONIC SIGNATURES CREATE A PRESUMPTION THAT THE SECURE ELECTRONIC SIGNATURE IS THE SIGNATURE OF THE PERSON TO WHOM IT CORRELATES AND THE SECURE ELECTRONIC SIGNATURE WAS AFFIXED BY THAT PERSON WITH THE INTENTION OF SIGNING OR APPROVING THE ELECTRONIC RECORD. THERE IS NO SUCH PRESUMPTION WHEN A NON-TRUSTWORTHY CERTIFICATE IS USED.

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

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

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

If there is any direct conflict between the Singapore CPS and any terms contained in the General CPS that are not resolved explicitly on the face of those documents, then the terms of the Singapore CPS will control, but only to the extent of that conflict. If a particular subject is addressed in this Singapore CPS and not in the General CPS, then the terms in this Singapore CPS will control.

1.2 Document Name and Identification

This document is the GlobalSign Certification Practice Statement for Certificates issued under Singapore Law and is identified by the Object Identifier 1.3.6.1.4.1.4146.3.65.

1.3 PKI Participants

1.3.1 Certification Authorities

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

Certificates including the policy identifier of Section 1.2 and issued from the following Certificate Authorities are in scope of this CPS:

Category	Name	Fingerprint
Generic	GlobalSign Root CA – R1	EBD41040E4BB3EC742C9E381D31EF2A41A48B6685C96E7CEF3C1DF6CD4331C99
	GlobalSign Root CA – R3	CBB522D7B7F127AD6A0113865BDF1CD4102E7D0759AF635A7CF4720DC963C53B
	GlobalSign Root CA – R5	179FBC148A3DD00FD24EA13458CC43BFA7F59C8182D783A513F6EBEC100C8924
	GlobalSign Root CA – R6	2CABEAFE37D06CA22ABA7391C0033D25982952C453647349763A3AB5AD6CCF69
	GlobalSign Root CA – R46	4FA3126D8D3A11D1C4855A4F807CBAD6CF919D3A5A88B03BEA2C6372D93C40C9
	GlobalSign Root CA – E46	CBB9C44D84B8043E1050EA31A69F514955D7BFD2E2C6B49301019AD61D9F5058
S/MIME	GlobalSign Secure Mail Root R45	319AF0A7729E6F89269C131EA6A3A16FCD86389FDCAB3C47A4A675C161A3F974
	GlobalSign Secure Mail Root E45	5CBF6FB81FD417EA4128CD6F8172A3C9402094F74AB2ED3A06B4405D04F30B19
Code Signing	GlobalSign Code Signing Root R45	7B9D553E1C92CB6E8803E137F4F287D4363757F5D44B37D52F9FCA22FB97DF86
	GlobalSign Code Signing Root E45	26C6C5FD4928FD57A8A4C5724FDD279745869C60C338E262FFE901C31BD1DB2B
Document Signing	GlobalSign Document Signing Root R45	38BE6C7EEB4547D82B9287F243AF32A9DEEB5DC5C9A87A0056F938D91B456A5A
	GlobalSign Document Signing Root E45	F86973BDD0514735E10C1190D0345BF89C77E1C4ADBD3F65963B803FD3C9E1FF
Timestamping	GlobalSign Timestamping Root R45	2BCBBFD66282C680491C8CD7735FDBBAB7A8079B127BEC60C535976834399AF7

Category	Name	Fingerprint
	GlobalSign Timestamping Root E46	4774674B94B78F5CCBEF89FDDEBDABBD894A71B55576B8CC5E6876BA3EAB4538
Client Authentication	GlobalSign Client Authentication Root R45	165C7E810BD37C1D57CE9849ACCD500E5CB01EEA37DC550DB07E598AAD2474A8
	GlobalSign Client Authentication Root E45	8B0F0FAA2C00FE0532A8A54E7BC5FD139C1922C4F10F0B16E10FB8BE1A634964

1.3.2 Registration Authorities

Identification and authentication of Applicants for Certificates is performed by a Registration Authority (RA). In addition, a Registration Authority may also initiate or pass along revocation requests for Certificates and requests for renewal and re-key of Certificates.

GlobalSign acts 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.
- Using officially notarized or otherwise authorized documents or sources of information to evaluate and authenticate an Applicant's application.
- Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and
- Initiating the process to revoke a Certificate.

Third Parties who enter a contractual relationship with GlobalSign may operate their own RA and authorize the issuance of Certificates. Third parties must minimally comply with all the requirements of this CPS and the terms of their contract which may also incorporate additional criteria.

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. If the RA relies on Certificates issued by third party Certification Authorities, RA is advised to review additional information by referring to such third party's CPS.

1.3.2.1 Local Registration Authorities

GlobalSign may designate an Organization as Local Registration Authority (LRA) or Enterprise RA to verify Certificate Requests from the Organization in accordance with section 1.3.2 of the GlobalSign CP.

1.3.3 Subscribers

See definition of "Subscriber" in Section 1.6.1 Definitions.

1.3.4 Relying Parties

See definition of "Relying Party" in Section 1.6.1 Definitions.

1.3.5 Other Participants

No Stipulation

1.4 Certificate Usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1 Appropriate Certificate Usage

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

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.

The appropriate certificate usage is defined by the Certificate Policy, indicated by the Certificate Policy Object Identifier.

1.4.2 Prohibited Certificate usage

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

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.

Certificates issued under this CPS may not be used:

- For any application requiring fail safe performance
- For any application or mechanism where issues with the certificate could cause a safety risk (e.g., human, or environmental risk)
- Where prohibited by law

1.5 Policy Administration

1.5.1 Organization Administering the Document

Requests for information or other inquiries associated with this CPS should be addressed to:

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

1.5.2 Contact Person

General Inquiries
GMO GlobalSign Pte. Ltd
attn. Legal Practices,
1 Wallich Street #25-01A,
Guoco Tower,
Singapore
Tel: + 65 (0) 3158 0349
Fax: + 65 (0) 6500 6366
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 4.9.3 for details of actions performed by GlobalSign for making this decision.

1.5.3 Person Determining CPS Suitability for the Policy

The GlobalSign PMA determines the suitability and applicability of this CP/CPS and the conformance based on the results and recommendations received from a Qualified Auditor.

1.5.4 CPS Approval Procedures

The GlobalSign PMA approves any revisions to this CPS document after formal review.

1.6 Definitions and Acronyms

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

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

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

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

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

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a base domain name and may use any one of the intermediate values for the purpose of domain validation.

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

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

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

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

Controller: the Controller appointed under section 27(1) and includes a Deputy or an Assistant Controller appointed under section 27(3) of the Singapore Electronic Transactions Act 2010.

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

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

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

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

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

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

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

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 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.

General CPS: GlobalSign's Certification Practice Statement available at http://www.globalsign.com/repository/ as updated from time to time.

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 Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

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.

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.

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

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

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

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created

with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Validation Specialist: Someone who performs the information verification duties.

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

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.

API	Application Programming Interface
ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EKU	Extended Key Usage
ETA	Electronic Transactions Act 2010
ETR	Electronic Transactions (Certification Authority) Regulations 2010
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force

ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration 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
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security

2.0 Publication and Repository Responsibilities

2.1 Repositories

This document, the GlobalSign CP, CPS and Subscriber Agreement are published on the public repositories: https://www.globalsign.com/repository and https://www.globalsign.com/en/company/corporate-policies.

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

In the event of any inconsistency, the English language version shall prevail.

2.2 Publication of Certificate Information

Records of all GlobalSign root certificates are available in the Certificate Repository:

https://www.globalsign.com/en/repository

Certificates contain URLs to locations where certificate-related information is published, including revocation information via OCSP and/or CRLs.

2.3 Time or Frequency of Publication

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

New or updated GlobalSign root and intermediate certificates are made publicly available as soon as possible. This typically means within seven days of creation.

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

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

For Certificate revocation requests, GlobalSign acts as an RA and authenticates the requests of parties wishing to revoke Certificates.

3.1 Naming

3.1.1 Types of Names

Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 and RFC-822 naming. DNs respect name space uniqueness and are not misleading.

3.1.2 Need for Names to be Meaningful

Certificates include a Subject field which identifies the subject entity (i.e., organization or domain). The Subject entity is identified using a distinguished name.

Certificates include an Issuer field which identifies the issuing entity. The issuing entity is identified using a distinguished name.

3.1.3 Anonymity or Pseudonymity of Subscribers

GlobalSign does not issue certificates with a natural person subject without a Subscriber's identity.

GlobalSign reserves the right to disclose the identity of the Subscriber if required by law.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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.

3.2 Initial Identity Validation

GlobalSign performs identification of the Applicant using any legal means of communication or investigation necessary to identify the Individual or Legal Entity.

If a certificate is issued to an individual ("new certificate") on the basis of another valid certificate held by the same individual ("originating certificate") and subsequently the originating certificate has been suspended or revoked, Subscriber is obligated to inform GlobalSign about the changed status of the Certificate. Upon such notice, GlobalSign will conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.

3.2.1 Method to Prove Possession of Private Key

No Stipulation.

3.2.2 Authentication of Organization identity

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 using the methods outlined below.

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

This information is verified using the validation methods defined in the GlobalSign CP.

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 Enterprise RA 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 can authenticate individuals under contract, all domains to be authenticated will have previously been verified by GlobalSign).

3.2.2.2 Role Based Certificate Authentication

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.

3.2.3 Authentication of Individual identity

GlobalSign authenticates Subscribers depending upon the class of Certificate as indicated below, in accordance with the validation methods defined in section 3.2.3 of the GlobalSign CP.

In addition to the methods below, GlobalSign may request further information from the Applicant. Other information and/or methods may be utilized to demonstrate an equivalent level of confidence.

GlobalSign does not authenticate additional information/attributes which may be provided by the Applicant during the application and enrollment process.

3.2.3.1 Class 1

This class covers Certificates for devices, natural persons and legal persons with only domain name and/or email address information.

The Applicant is required to demonstrate control of their email address and/or domain name to which the Certificate relates.

3.2.3.2 Class 2

This class covers Certificates for natural persons (with and without affiliation to an organization), validated to a medium level.

If Class 1 information is included, the information is validated in accordance with Class 1.

3.2.3.2.1 Natural person (without affiliation)

The individual 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 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.

3.2.3.2.2 Natural person (affiliated to an organization)

GlobalSign authenticates the individual's identity through one of the following methods:

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

3.2.3.3 Class 3

This class covers Certificates for natural persons (with and without affiliation to an organization), validated to a high level.

The individual 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.

A face-to-face meeting is required to establish the individual's identity with an attestation from the notary or trusted third party that they have met the individual and have inspected their national photo ID document, and that the application details for the order are correct. GlobalSign may establish the Individual's identity and perform inspection of a Governmentally Accepted Form of ID through a video-based meeting or an approach with equivalent assurance

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 GlobalSign CP.

If Class 1 or Class 2 information is included, the information is validated in accordance with the sections above.

3.2.4 Non-Verified Subscriber Information

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

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

3.2.5 Validation of Authority

If the Applicant for a Certificate request is an Organization, the request must be made by an individual authorized to act on behalf of the Organization (authorized representative).

GlobalSign shall verify the authority of an individual to act on behalf of the Organization using one or more of the following methods:

- Verification through a reliable means of communication with the organization.
- Verification through a reliable source that indicates affiliation of the individual with the organization.

3.2.6 Criteria for Interoperation

As per 2.1.

3.2.7 Authentication of Domain Names

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 in accordance with Section 3.2.7.1 of the GlobalSign CP.

3.2.8 Authentication of IP Addresses

GlobalSign uses the methods in Section 3.2.7.2 of the GlobalSign CP to confirm that the Applicant (or the Applicant's parent company's, subsidiary company's, or Affiliate's, collectively referred to as "Applicants" for the purposes of this section) has control of or right to use IP addresses.

3.2.9 Authentication of Email Addresses

GlobalSign uses the methods in Section 3.2.8 of the GlobalSign CP to confirm that the Applicant (or the Applicant's parent company's, subsidiary company's, or Affiliate's, collectively referred to as "Applicants" for the purposes of this section) has control of or right to use email addresses.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

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

Identification of the request is subject to the conditions specified in Section 3.2. If at any point any information included in a Certificate is changed in any way, additional validation must be performed.

3.3.2 Identification and Authentication for Re-key After Revocation

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

3.4 Identification and Authentication for Revocation Request

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.

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

Applications are accepted via one of three methods:

- **On-line** Via a web interface over an https session. An Applicant must apply via a secure ordering process according to a procedure maintained by GlobalSign. Most direct customers use this method. 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 partner or reseller.
- **API** Applicants can submit an appropriately formatted Certificate Request via an approved API to GlobalSign with suitably strong credentials. The account may be classified as API.
- **Manual** Applicants with custom requests 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.

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

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

Approval requires successful completion of validation per Section 3.2.

GlobalSign maintains its own blocklists 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 for screening Applicants.

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

4.2.3 Time to Process Certificate Applications

GlobalSign shall ensure that all reasonable methods are used to evaluate and process Certificate applications. Certificate requests are typically processed within 24-96 hours. Where issues outside of the control of GlobalSign occur, GlobalSign shall strive to keep the Applicant duly informed.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Prior to certificate issuance, GlobalSign ensures that information to be included in the certificate is validated in accordance with Section 3.2. The certificate is then submitted for signing by the applicable CA. After issuance, the certificate is stored in a database and made available to Subscriber.

Certificates issued by the Root CA require an individual authorized by GlobalSign to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

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.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

GlobalSign publishes the Certificate by delivering it to the Subscriber and may also publish to one or more Certificate Transparency Logs. Certificates are not published to another repository unless agreed differently between GlobalSign and Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties.

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.

Separate key pairs must exist for digital signature and encryption.

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 lifecycle of a Private Key, Subscribers must securely delete all copies of the Private Key.

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.

Relying Party must accept and act in accordance with the requirements in Section 9.6.4 prior to reliance upon a Certificate from GlobalSign. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made.

Software used by Relying Parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate Renewal

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

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

4.6.1 Circumstances for Certificate Renewal

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

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

To process a renewal request, GlobalSign verifies the request with Subscriber or their authorized representative.

Certificate renewal requests are processed as new Certificate requests.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

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

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

4.7.1 Circumstances for Certificate Re-Key

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

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

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-Keying Requests

To process a re-key request, GlobalSign verifies the request with Subscriber or their authorized representative.

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

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

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

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

4.8.1 Circumstances for Certificate Modification

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

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

To process a modification request, GlobalSign verifies the request with Subscriber or their authorized representative.

Certificate modification requests are processed as new Certificate requests.

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Prior to performing a revocation GlobalSign will verify the authenticity of the revocation request.

GlobalSign may revoke any Certificate at its sole discretion and shall revoke a Certificate, regardless of whether the subscriber listed in the certificate consents, if GlobalSign confirms that:

a) a material fact represented in the certificate is false
b) a requirement for issuance of the certificate was not satisfied
c) GlobalSign's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability
d) an individual subscriber is dead; or
e) a subscriber has been dissolved, wound up or otherwise ceased to exist.

Upon effecting such a revocation, other than in case (d) or (e), GlobalSign immediately notifies the subscriber listed in the revoked certificate.

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 circumstances documented in Section 4.9.1 of the CP and:

1. Information within the Certificate marked with extension "critical" is inaccurate.
2. Private key or media holding the private key is suspected or compromised.
3. Subscriber is no longer a member of the community subject to the GlobalSign CP.
4. Subscriber requests revocation of the Certificate.
5. Suspected or actual violations of the generation or issuance process.
6. Suspected or confirmed compromise of the CA private key
7. Revocation is required by GlobalSign's CP and/or this CPS.

Revocation of a Subscriber Certificate is performed within a commercially reasonable time under the circumstances documented in Section 4.9.1 of the GlobalSign CP.

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

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

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

Revocation of a Subordinate CA Certificate is performed within seven (7) days under the circumstances documented in Section 4.9.1 of the GlobalSign CP.

4.9.2 Who Can Request Revocation

Prior to performing a revocation GlobalSign will verify the authenticity of the revocation request.

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, an agent of the Subscriber with authority to request the revocation 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.

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 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 account. Alternatively, where 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.

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 Problem Report via report-abuse@globalsign.com. GlobalSign may or may not revoke in response to this request. See section 4.9.5 for detail of actions performed by GlobalSign for making this decision.

GlobalSign informs the Subscriber of a revoked certificate typically within 1 hour of revocation.

4.9.4 Revocation Request Grace Period

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

Subscribers must inform GlobalSign within 48 hours of a key compromise.

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 will be processed within a maximum of 24 hours of receipt.

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, otherwise all warranties become void.

Relying Parties will need to consult the CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI).

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

Relying Parties must verify the validity of Certificates via CRL or OCSP prior to relying on Certificates. Respective CRL and OCSP location information are provided within Certificates.

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

4.9.7 CRL Issuance Frequency

For the status of Subscriber Certificates:
For CAs that publish a CRL, the CRL will be updated and re-issued at least once every seven days, and the value of the nextUpdate field will not be more than ten days beyond the value of the thisUpdate field.

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

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

GlobalSign OCSP responses conform 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. Each OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

For the status of Subscriber Certificates:

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

For the status of Subordinate CA Certificates:

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

GlobalSign and any of its Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where GlobalSign at its own discretion decides that evidence suggests a possible Key Compromise has taken place.

4.9.13 Circumstances for Suspension

GlobalSign may suspend a certificate that it has issued if there are reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension.

In these circumstances, GlobalSign shall complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate.

GlobalSign shall suspend a certificate after receiving a valid request for suspension, however if revocation is justified in the light of all the evidence available to it, the certificate will be revoked.

4.9.14 Who Can Request Suspension

Unless agreed otherwise between GlobalSign and the Subscriber, GlobalSign shall suspend a certificate as soon as possible after receiving a request by a person whom GlobalSign believes to be:

a) the subscriber listed in the certificate;
b) a person duly authorized to act for that subscriber; or
c) a person acting on behalf of that subscriber, who is unavailable.

4.9.15 Procedure for Suspension Request

A request for suspension may be submitted using e-mail, API or a customer certificate management panel provided by GlobalSign.

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 in accordance with Section 4.10.1 of the GlobalSign CP.

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.

Upon system failure, service or other factors which are not under the control of GlobalSign, GlobalSign aims to ensure that this information service is not unavailable for longer than 48 hours.

4.10.3 Operational Features

No stipulation

4.11 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are 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

5.1 Physical Controls

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 on-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 before being released for disposal.

5.1.8 Off-Site Backup

As stipulated in section 5.5.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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.
- **Validation Specialists:** 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.
- **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 (logically) or procedurally or a combination of 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. (Validation Specialists)
- Those performing installation, configuration, and maintenance of the CA systems. (Infra system engineer)
- Those with overall responsibility for administering the implementation of the CA’s security practices. (Security Officer)
- Those performing duties related to cryptographic key life cycle management (e.g., key component custodians). (CA activation data holders)
- Those performing CA systems development. (Developers)
- Those performing CA systems auditing (Infra Operator, Auditor)

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

GlobalSign employs personnel that possesses 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 analyzed, provided such checks are permitted by the jurisdiction in which the person will be employed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation where permitted by law.

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

5.3.3 Training Requirements

GlobalSign maintains training programs for each role and maintains records of such training.

5.3.4 Retraining Frequency and Requirements

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

GlobalSign provides information security and privacy training at least once a year for each role.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions are applied to personnel violating GlobalSign's operational procedures and policies.

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 practice statement, any corresponding CP, and any relevant statutes, policies, or contracts.

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

GlobalSign makes and stores in a trustworthy manner the records relating to:

(a) activities in issuance, renewal, suspension, and revocation of certificates (including the process of identification of any person requesting a certificate from an accredited certification authority).
(b) the process of generating subscribers' (where applicable) or the accredited certification authority's own key pairs.
(c) the administration of an accredited certification authority's computing facilities; and
(d) such critical related activity of an accredited certification authority as may be determined by the Controller.

The date and time of all transactions in relation to the issuance, renewal, suspension and revocation of a certificate is logged and stored in a trustworthy manner.

Additionally, the following audit trails are recorded:

- Application transactions:
    - Registration
    - Certification
    - Publication
    - Suspension
    - Revocation
- System log files:
    - Security violations
    - Errors
    - Execution of privilege functions
    - Changes in access control and system configurations

GlobalSign will make these records available to its Auditor upon request.

5.4.2 Frequency of Processing Log

No stipulation.

5.4.3 Retention Period for Audit Log

GlobalSign retains any audit logs generated for at least 7 years and up to 10 years and will make these audit logs available to its Auditor upon request.

5.4.4 Protection of Audit Log

Events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

The records of events are protected to prevent alteration and detect tampering and to ensure that only individuals with authorized 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 realization.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System

Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects the data confidentiality. In 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.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

GlobalSign performs annual risk assessment in accordance with Section 5.4.8 of the GlobalSign CP.

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

5.5 Records Archival

5.5.1 Types of Records Archived

GlobalSign and RAs archive items identified in Section 5.4.1 and may archive any further data to ensure proper operation of the CA.

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.

The retention period is at least 7 years and up to 10 years after any Certificate based on that documentation ceases to be valid, unless specified otherwise in an agreement with GlobalSign.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

Archived are backed-up regularly and stored at an off-site location with at least the same level of security as the primary location.

5.5.5 Requirements for Timestamping of Records

GlobalSign timestamps all logs indicating the time at which the event occurred, either through a digital or manual timestamp.

5.5.6 Archive Collection System (Internal or External)

No Stipulation

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized 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 changeover key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may also be modified, and Certificate profiles may be altered to adhere to best practices. Private Keys used to sign previous Subscriber Certificates 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 maintains incident response and disaster recovery plans and procedures in accordance with Section 5.7.1 of the GlobalSign CP.

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.

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

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

5.7.3 Entity Private Key Compromise Procedures

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

If so, then:

- All the Subscribers who have been issued a Certificate from this hierarchy will be notified at the earliest feasible opportunity; and
- A new CA Private Key and Certificate shall be generated, or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.
- If a new CA has been created, the CA public key shall be published on the public repository.

5.7.4 Availability of revocation status

Revocation status information will be provided and maintained at a publicly accessible location in case of CA key compromise, including, if applicable, transferring Certificate status information services to another GMO Internet Group entity.

5.7.5 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 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 minimized as much as possible.
- ensure that archived records of the Issuing CA are retained.
- ensure that prompt notification of termination is provided to Subscribers, Authorized Relying Parties, Application Software Providers, and other relevant stakeholders in GlobalSign certificate lifecycles.
- ensure Certificate status information services are provided and maintained for the applicable period after termination, including, if applicable, transferring Certificate status information services to another 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 the Controller and auditors; and
- notify other relevant Government and Certification bodies under applicable laws and related regulations.

5.8.1 Successor Issuing Certification Authority

To the extent that it is practical and reasonable, the successor Issuing CA should assume the same rights, obligations, and duties as the terminating Issuing CA. The successor Issuing CA should issue new Keys and Digital Certificates to all Subscribers whose Keys and Digital Certificates were revoked by the terminating Issuing CA due to its termination, subject to the Subordinate CA or User making an application for a new Digital Certificate and satisfying the initial registration and Identification and Authentication requirements, including the execution of new agreements.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

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

For CA Key Pairs used for public Root or Subordinate CA Certificates, GlobalSign also performs the following:

1. prepare and follow a Key Generation Script;
2. generate the CA Key Pair in a physically secured environment as described in the GlobalSign's CP and this CPS;
3. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
4. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in GlobalSign's CP and this CPS;
5. log its CA Key Pair generation activities; and
6. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate

Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

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 (or equivalent) using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

For Subscriber key pairs generated by the Subscriber, the key generation system must be approved by GlobalSign.

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

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.

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

6.1.3 Public Key Delivery to Certificate Issuer

GlobalSign 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.

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

GlobalSign follows NIST Special Publication 800-133 Revision 2 (2020) - Recommendation for Cryptographic Key Generation for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Issuing CAs and end entity Certificates delivered to Subscribers.

Minimum requirements of key sizes are applied in accordance with Section 6.1.5 of the GlobalSign CP.

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.

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.
3. 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.

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).

6.2.3 Private Key Escrow

GlobalSign does not escrow Private Keys.

6.2.4 Private Key Backup

If required for business continuity GlobalSign backs up Root CA and Subordinate CA Private Keys under the same multi-person control as the original Private Key.

For products where backup of Subscriber Private Keys is performed, these keys are stored with the same security controls as the original.

6.2.5 Private Key Archival

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

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

6.2.7 Private Key Storage on Cryptographic Module

GlobalSign stores 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 CA 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.

Subscriber Private Keys generated by GlobalSign in GCC are stored in PKCS#12 format and after 30 days have passed after the key generation, the Subscriber Key Pair is automatically deleted from GCC.

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

No Stipulation

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

CA Certificates have a maximum Validity Period of:

Type	Private Key Usage	Max Validity Period
Root CAs[1]	No stipulation	28 years
Subordinate CAs	No stipulation	18 years

The Key Pair usage period can be up to the Certificate Validity Period. Certificates signed by a specific CA must expire before or at the end of that CA Certificate Validity period.

Subscriber certificate validity periods are in accordance with Section 6.3.2 of the GlobalSign CP.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of GlobalSign activation data used to activate GlobalSign CA 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.

---

[1] *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.*

6.4.2 Activation Data Protection

GlobalSign CA private key 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 CA private key activation data may only be held by GlobalSign personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

- Systems performing certification functions are not used for general purposes (e.g. word processing, emailing, web surfing)
- Strong password policies are implemented
- Inactive lockouts are implemented
- Updated security patches are reviewed, tested, applied and implemented.
- Authenticated logins for trusted roles.
- Access control with least privilege.
- Means for malicious code protection.
- Security audit capability, protected in integrity.

6.5.2 Computer Security Rating

No Stipulation

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

System development controls for CA systems are as follows:

- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. Commercial off-the-shelf hardware and software must meet minimum security and quality levels and is subject to a vendor selection process.
- Hardware will be inspected during the commissioning process to ensure conformity of the supplied hardware, and to confirm the hardware has not been tampered with. Hardware and software procured are procured using controls to reduce the likelihood of tampering.
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operations.
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are installed on the equipment and are obtained from sources authorized by local policy. 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 GlobalSign CA systems as well as any modifications and upgrades are documented and controlled. Controls are in place for detecting unauthorized modification to GlobalSign software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of GlobalSign CA systems. Software, when first loaded,

is checked as being supplied from the vendor, with no modifications, and to confirm if it is the version intended for use.

6.6.3 Lifecycle Security Controls

No Stipulation

6.7 Network Security Controls

GlobalSign implements appropriate security measures to ensure:

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

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.

Subordinate CA and end entity certificates include an Extended Key Usage extension containing KeyPurposeId(s) describing the intended usage(s) of the certificate. The KeyPurposeId anyExtendedKeyUsage is not included in publicly trusted end entity certificates.

7.1.3 Algorithm Object Identifiers

GlobalSign issues Certificates with algorithms indicated by the following OIDs:

SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
SHA512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

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

7.1.4 Name Forms

No Stipulation

7.1.5 Name Constraints

No Stipulation

7.1.6 Certificate Policy Object Identifier

Certificate Policy OIDs are included in accordance with section 7.1.6 of the GlobalSign CP.

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 one or more Policy Qualifiers with reference to the CPS URI and may include a userNotice 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 issues 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.

7.2 CRL Profile

7.2.1 Version Number(s)

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

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

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

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

Following extensions are supported:

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

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

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

7.3 OCSP Profile

GlobalSign operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 and RFC 5019 and includes the OCSP responder URL within issued certificates' AIA extension.

7.3.1 Version Number(s)

GlobalSign issues Version 1 OCSP responses.

7.3.2 OCSP Extensions

No stipulation.

8.0 Compliance Audit and Other Assessments

The procedures within this CPS are designed to comply with the requirements listed in Section 1.0 and encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which GlobalSign operates.

8.1 Frequency and Circumstances of Assessment

GlobalSign maintains its compliance with the Electronic Transactions Act 2010 and Electronic Transactions (Certification Authority) Regulations 2010 via a Qualified Auditor every 2 years.

8.2 Identity/Qualifications of Assessor

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

- Independence from the subject of the audit.
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8.0 of this document.
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function.
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme.
- Bound by law, government regulation, or professional code of ethics; and
- 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.

8.3 Assessor’s Relationship to Assessed Entity

GlobalSign selected an assessor who is completely independent from GlobalSign.

8.4 Topics Covered by Assessment

The audit meets the requirements of the audit schemes highlighted in Section 1.0 under which the assessment is being made. These requirements may vary as audit schemes are updated. 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

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

8.6 Communications of Results

Results of the audit are reported to the Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan. GlobalSign will submit the report to the Controller within 4 weeks of the availability of the report.

The results could also be made available to any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement.

8.7 Self-Audit

GlobalSign monitors its adherence to GlobalSign CP, this CPS 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 in accordance with Section 8.7 of the GlobalSign CP.

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 re-reissuance Fees and any associated terms and conditions are made clear to Applicants both by the enrollment process through a web interface or in the sales and marketing materials on GlobalSign's various language specific web sites.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

GlobalSign may charge additional fees to Subscribers who have a large Relying Party community and choose not to use OCSP stapling or other similar techniques to reduce the load on the GlobalSign's Certificate status infrastructure.

9.1.4 Fees for Other Services

GlobalSign may charge for other additional services such as timestamping.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

GlobalSign 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

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by GlobalSign staff including Validation Specialists 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

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

GlobalSign protects personal information in accordance with a Privacy Policy published on GlobalSign's 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.

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. 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.

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, in issuing and managing the Certificate and in verifying the accuracy of the information contained in the Certificate, GlobalSign has complied with its Certificate Policy and/or Certification Practice Statement.

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

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.

9.6.4 Relying Party Representations and Warranties

Prior to relying on a Certificate, Relying Parties must accept and act in accordance with the requirements of this CPS.

A party relying on a Certificate represents and warrants to:

- Have the technical capability to use Certificates.
- Receive notice of the Issuing CA and associated conditions for Relying Parties.
- Verify the authenticity and validity of a certificate by verifying at least the following:
    - Issuing CA signature
    - Certificate policy parameters
    - Certificate usage parameters
    - Certificate validity period
    - Revocation or suspension information
    - Certificate reliance limit
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CPS.
- 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.
- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party.
- Validate a 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 a 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 a 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.

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.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

OTHER THAN AS PROVIDED HEREIN OR WHERE PROHIBITED BY LAW, THE CERTIFICATES ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND GLOBALSIGN DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. GLOBALSIGN DOES NOT WARRANT THAT ANY CERTIFICATE WILL MEET SUBSCRIBER'S OR ANY OTHER PARTY'S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE UNINTERRUPTED OR ERROR-FREE. E

9.8 Limitations of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY, GLOBALSIGN'S TOTAL LIABILITY TO A SUBSCRIBER OR RELYING PARTY ARISING OUT OF OR RELATING TO USE OR RELIANCE ON A CERTIFICATE ISSUED UNDER THIS CPS WILL NOT EXCEED ONE HUNDRED DOLLARS ($100) PER CALIM PER CERTIFICATE WITH AN AGGREGATE TOTAL OF ONE THOUSAND DOLLARS ($1,000) PER CERTFICATE REGARDLESS OF THE METHOD OF APPORTIONMENT AMONG CLAIMANTS OR THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO A CERTIFICATE.

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

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify GlobalSign, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this 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.

9.9.2 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 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

This CPS is reviewed at least annually and may be reviewed more frequently. All changes are reviewed and approved by the GlobalSign CA Governance Policy Authority before insertion. Approval from the Controller is required before publication of the CPS.

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 effective. Any updates become binding for all Certificates that have been issued or are to be issued upon the effective date of the updated version of this document.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

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

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

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration, shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre ("SIAC") in accordance with the Arbitration Rules of the Singapore International Arbitration Centre ("SIAC Rules") for the time being in force, which rules are deemed to be incorporated by reference in this clause.

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 Singapore and the arbitrators determine all associated costs.

9.14 Governing Law

This CPS is governed, construed, and interpreted in accordance with the laws of Singapore. 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 Singapore 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.

9.15 Compliance with Applicable Law

GlobalSign complies with applicable laws of Singapore. 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 Singapore.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

GlobalSign requires parties using GlobalSign products and services to enter into an agreement that details the specific terms for the applicable product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce 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

No Stipulation