GlobalSign CA
Certification Practice Statement

Date: 2nd September 2014

Version: v7.8

Table of Contents

TABLE OF CONTENTS **2**

DOCUMENT HISTORY **7**

DETAILED HISTORY OF CHANGES **7**

ACKNOWLEDGMENTS **9**

1.0 INTRODUCTION **10**

1.1 OVERVIEW 10
1.1.1 Certificate Naming *12*
1.2 DOCUMENT NAME AND IDENTIFICATION 13
1.3 PKI PARTICIPANTS 14
1.3.1 Certification Authorities *14*
1.3.2 Registration Authorities *14*
1.3.3 Subscribers *15*
1.3.4 Relying Parties *15*
1.3.5 Other Participants *15*
1.4 CERTIFICATE USAGE 16
1.4.1 Appropriate certificate usage *16*
1.4.2 Prohibited Certificate usage *18*
1.5 POLICY ADMINISTRATION 19
1.5.1 Organization Administering the Document *19*
1.5.2 Contact Person *19*
1.5.3 Person Determining CPS Suitability for the Policy *20*
1.5.4 CPS Approval Procedures *20*
1.6 DEFINITIONS AND ACRONYMS 20

2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES **25**

2.1 REPOSITORIES 25
2.2 PUBLICATION OF CERTIFICATE INFORMATION 25
2.3 TIME OR FREQUENCY OF PUBLICATION 25
2.4 ACCESS CONTROL ON REPOSITORIES 25

3.0 IDENTIFICATION AND AUTHENTICATION **26**

3.1 NAMING 26
3.1.1 Types of Names *26*
3.1.2 Need for Names to be Meaningful *26*
3.1.3 Anonymity or Pseudonymity of Subscribers *26*
3.1.4 Rules for Interpreting Various Name Forms *26*
3.1.5 Uniqueness of Names *26*
3.1.6 Recognition, Authentication, and Role of Trademarks *27*
3.2 INITIAL IDENTITY VALIDATION 27
3.2.1 Method to Prove Possession of Private Key *27*
3.2.2 Authentication of Organization Identity *27*
3.2.3 Authentication of Individual identity *28*
3.2.4 Non-Verified Subscriber Information *30*
3.2.5 Validation of Authority *30*
3.2.6 Criteria for Interoperation *31*
3.2.7 Authentication of Domain Name *31*
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 32
3.3.1 Identification and Authentication for Routine Re-key *32*
3.3.2 Identification and Authentication for Reissuance after Revocation *33*
3.3.3 Re-verification and Revalidation of Identity When Certificate Information Changes *33*
3.3.4 Identification and Authentication for Re-key After Revocation *33*
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 33

4.0 CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS 33

4.1 CERTIFICATE APPLICATION 33
4.1.1 Who Can Submit a Certificate Application 33
4.1.2 Enrollment Process and Responsibilities 34
4.2 CERTIFICATE APPLICATION PROCESSING 34
4.2.1 Performing Identification and Authentication Functions 34
4.2.2 Approval or Rejection of Certificate Applications 34
4.2.3 Time to Process Certificate Applications 35
4.3 CERTIFICATE ISSUANCE 35
4.3.1 CA Actions during Certificate Issuance 35
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate 35
4.3.3 Notification to North American Energy Standards Board (NAESB) Subscribers by the CA of Issuance of Certificate 35
4.4 CERTIFICATE ACCEPTANCE 36
4.4.1 Conduct Constituting Certificate Acceptance 36
4.4.2 Publication of the Certificate by the CA 36
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 36
4.5 KEY PAIR AND CERTIFICATE USAGE 36
4.5.1 Subscriber Private Key and Certificate Usage 36
4.5.2 Relying Party Public Key and Certificate Usage 36
4.6 CERTIFICATE RENEWAL 36
4.6.1 Circumstances for Certificate Renewal 36
4.6.2 Who May Request Renewal 37
4.6.3 Processing Certificate Renewal Requests 37
4.6.4 Notification of New Certificate Issuance to Subscriber 37
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 37
4.6.6 Publication of the Renewal Certificate by the CA 37
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 37
4.7 CERTIFICATE RE-KEY 37
4.7.1 Circumstances for Certificate Re-Key 37
4.7.2 Who May Request Certification of a New Public Key 38
4.7.3 Processing Certificate Re-Keying Requests 38
4.7.4 Notification of New Certificate Issuance to Subscriber 38
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 38
4.7.6 Publication of the Re-Keyed Certificate by the CA 38
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 38
4.8 CERTIFICATE MODIFICATION 38
4.8.1 Circumstances for Certificate Modification 38
4.8.2 Who May Request Certificate Modification 38
4.8.3 Processing Certificate Modification Requests 38
4.8.4 Notification of New Certificate Issuance to Subscriber 38
4.8.5 Conduct Constituting Acceptance of Modified Certificate 38
4.8.6 Publication of the Modified Certificate by the CA 38
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 38
4.9 CERTIFICATE REVOCATION AND SUSPENSION 39
4.9.1 Circumstances for Revocation 39
4.9.2 Who Can Request Revocation 40
4.9.3 Procedure for Revocation Request 40
4.9.4 Revocation Request Grace Period 40
4.9.5 Time Within Which CA Must Process the Revocation Request 40
4.9.6 Revocation Checking Requirements for Relying Parties 41
4.9.7 CRL Issuance Frequency 41
4.9.8 Maximum Latency for CRLs 41
4.9.9 On-Line Revocation/Status Checking Availability 41
4.9.10 On-Line Revocation Checking Requirements 41
4.9.11 Other Forms of Revocation Advertisements Available 41

4.9.12 Special Requirements Related to Key Compromise 41
4.9.13 Circumstances for Suspension 41
4.9.14 Who Can Request Suspension 42
4.9.15 Procedure for Suspension Request 42
4.9.16 Limits on Suspension Period 42
4.10 CERTIFICATE STATUS SERVICES 42
4.10.1 Operational Characteristics 42
4.10.2 Service Availability 42
4.10.3 Operational Features 42
4.10.4 End of Subscription 42
4.11 KEY ESCROW AND RECOVERY 42
4.11.1 Key Escrow and Recovery Policy and Practices 42
4.11.2 Session Key Encapsulation and Recovery Policy and Practices 42

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 42

5.1 PHYSICAL CONTROLS 42
5.1.1 Site Location and Construction 42
5.1.2 Physical Access 43
5.1.3 Power and Air Conditioning 43
5.1.4 Water Exposures 43
5.1.5 Fire Prevention and Protection 43
5.1.6 Media Storage 43
5.1.7 Waste Disposal 43
5.1.8 Off-Site Backup 43
5.2 PROCEDURAL CONTROLS 43
5.2.1 Trusted Roles 43
5.2.2 Number of Persons Required per Task 43
5.2.3 Identification and Authentication for Each Role 44
5.2.4 Roles Requiring Separation of Duties 44
5.3 PERSONNEL CONTROLS 44
5.3.1 Qualifications, Experience, and Clearance Requirements 44
5.3.2 Background Check Procedures 44
5.3.3 Training Requirements 44
5.3.4 Retraining Frequency and Requirements 44
5.3.5 Job Rotation Frequency and Sequence 45
5.3.6 Sanctions for Unauthorized Actions 45
5.3.7 Independent Contractor Requirements 45
5.3.8 Documentation Supplied to Personnel 45
5.4 AUDIT LOGGING PROCEDURES 45
5.4.1 Types of Events Recorded 45
5.4.2 Frequency of Processing Log 45
5.4.3 Retention Period for Audit Log 45
5.4.4 Protection of Audit Log 45
5.4.5 Audit Log Backup Procedures 45
5.4.6 Audit Collection System (Internal vs. External) 46
5.4.7 Notification to Event-Causing Subject 46
5.4.8 Vulnerability Assessments 46
5.5 RECORDS ARCHIVAL 46
5.5.1 Types of Records Archived 46
5.5.2 Retention Period for Archive 47
5.5.3 Protection of Archive 47
5.5.4 Archive Backup Procedures 47
5.5.5 Requirements for Timestamping of Records 47
5.5.6 Archive Collection System (Internal or External) 47
5.5.7 Procedures to Obtain and Verify Archive Information 47
5.6 KEY CHANGEOVER 47
5.7 COMPROMISE AND DISASTER RECOVERY 47

5.7.1 Incident and Compromise Handling Procedures 47
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 48
5.7.3 Entity Private Key Compromise Procedures 48
5.7.4 Business Continuity Capabilities After a Disaster 48
5.8 CA OR RA TERMINATION 48

6.0 TECHNICAL SECURITY CONTROLS 48

6.1 KEY PAIR GENERATION AND INSTALLATION 48
6.1.1 Key Pair Generation 48
6.1.2 Private Key Delivery to Subscriber 48
6.1.3 Public Key Delivery to Certificate GlobalSign CA 48
6.1.4 CA Public Key Delivery to Relying Parties 49
6.1.5 Key Sizes 49
6.1.6 Public Key Parameters Generation and Quality Checking 49
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 49
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 49
6.2.1 Cryptographic Module Standards and Controls 49
6.2.2 Private Key (n out of m) Multi-Person Control 49
6.2.3 Private Key Escrow 49
6.2.4 Private Key Backup 49
6.2.5 Private Key Archival 49
6.2.6 Private Key Transfer Into or From a Cryptographic Module 50
6.2.7 Private Key Storage on Cryptographic Module 50
6.2.8 Method of Activating Private Key 50
6.2.9 Method of Deactivating Private Key 50
6.2.10 Method of Destroying Private Key 50
6.2.11 Cryptographic Module Rating 50
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 50
6.3.1 Public Key Archival 50
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 50
6.4 ACTIVATION DATA 51
6.4.1 Activation Data Generation and Installation 51
6.4.2 Activation Data Protection 51
6.4.3 Other Aspects of Activation Data 51
6.5 COMPUTER SECURITY CONTROLS 51
6.5.1 Specific Computer Security Technical Requirements 51
6.5.2 Computer Security Rating 51
6.6 LIFECYCLE TECHNICAL CONTROLS 51
6.6.1 System Development Controls 51
6.6.2 Security Management Controls 52
6.6.3 Lifecycle Security Controls 52
6.7 NETWORK SECURITY CONTROLS 52
6.8 TIME STAMPING 52
6.8.1 PDF Signing Time Stamping Services 52
6.8.2 Code Signing and EV Code Signing Time Stamping Services 52

7.0 CERTIFICATE, CRL, AND OCSP PROFILES 52

7.1 CERTIFICATE PROFILE 52
7.1.1 Version Number(s) 52
7.1.2 Certificate Extensions 53
7.1.3 Algorithm Object Identifiers 53
7.1.4 Name Forms 53
7.1.5 Name Constraints 53
7.1.6 Certificate Policy Object Identifier 53
7.1.7 Usage of Policy Constraints Extension 53
7.1.8 Policy Qualifiers Syntax and Semantics 53
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 53

7.2 CRL PROFILE 53
7.2.1 Version Number(s) *53*
7.2.2 CRL and CRL Entry Extensions *53*
7.3 OCSP PROFILE 53
7.3.1 Version Number(s) *53*
7.3.2 OCSP Extensions *54*

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 54

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT 54
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 54
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 54
8.4 TOPICS COVERED BY ASSESSMENT 54
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 54
8.6 COMMUNICATIONS OF RESULTS 55

9.0 OTHER BUSINESS AND LEGAL MATTERS 55

9.1 FEES 55
9.1.1 Certificate Issuance or Renewal Fees *55*
9.1.2 Certificate Access Fees *55*
9.1.3 Revocation or Status Information Access Fees *55*
9.1.4 Fees for Other Services *55*
9.1.5 Refund Policy *55*
9.2 FINANCIAL RESPONSIBILITY 55
9.2.1 Insurance Coverage *55*
9.2.2 Other Assets *55*
9.2.3 Insurance or Warranty Coverage for End Entities *55*
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 55
9.3.1 Scope of Confidential Information *55*
9.3.2 Information Not Within the Scope of Confidential Information *56*
9.3.3 Responsibility to Protect Confidential Information *56*
9.4 PRIVACY OF PERSONAL INFORMATION 56
9.4.1 Privacy Plan *56*
9.4.2 Information Treated as Private *56*
9.4.3 Information Not Deemed Private *56*
9.4.4 Responsibility to Protect Private Information *56*
9.4.5 Notice and Consent to Use Private Information *56*
9.4.6 Disclosure Pursuant to Judicial or Administrative Process *56*
9.4.7 Other Information Disclosure Circumstances *56*
9.5 INTELLECTUAL PROPERTY RIGHTS 56
9.6 REPRESENTATIONS AND WARRANTIES 56
9.6.1 CA Representations and Warranties *56*
9.6.2 RA Representations and Warranties *58*
9.6.3 Subscriber Representations and Warranties *58*
9.6.4 Relying Party Representations and Warranties *59*
9.7 DISCLAIMERS OF WARRANTIES 60
9.8 LIMITATIONS OF LIABILITY 60
9.9 INDEMNITIES 60
9.9.1 Indemnification by GlobalSign CA *60*
9.9.2 Indemnification by Subscribers *60*
9.9.3 Indemnification by Relying Parties *61*
9.10 TERM AND TERMINATION 61
9.10.1 Term *61*
9.10.2 Termination *61*
9.10.3 Effect of Termination and Survival *61*
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 61
9.12 AMENDMENTS 61
9.12.1 Procedure for Amendment *61*

9.12.2 Notification Mechanism and Period *61*
9.12.3 Circumstances Under Which OID Must be Changed *61*
9.13 DISPUTE RESOLUTION PROVISIONS 61
9.14 GOVERNING LAW 62
9.15 COMPLIANCE WITH APPLICABLE LAW 62
9.16 MISCELLANEOUS PROVISIONS 62
9.16.1 Compelled Attacks *62*
9.16.2 Entire Agreement *62*
9.16.3 Assignment *62*
9.16.4 Severability *62*
9.16.5 Enforcement (Attorney's Fees and Waiver of Rights) *62*
9.17 OTHER PROVISIONS 62

Document History

Version	Release Date	Author	Status + Description
V5.0 – V5.5	10/07/05 – 19/06/07	Various Authors	Various changes leading up to a rewrite to support Extended Validation
V5.6	25/06/07	Steve Roylance	Final modification for EV Issue 1.0
V6.0	17/12/07	Steve Roylance	Major Release supporting new Certificate life cycle solutions
V6.1	20/05/08	Steve Roylance	Administrative update/ clarifications
V6.2	13/10/08	Steve Roylance	Administrative update/ clarifications
V6.3	16/12/08	Steve Roylance	Administrative update/ clarifications
V6.4	11/02/09	Steve Roylance	Administrative update/clarifications
V6.5	12/05/09	Steve Roylance	Administrative update/clarifications
V6.6	03/02/10	Lila Kee	Administrative update
V6.7	12/05/10	Johan Sys	Administrative update/clarifications
V7.0	22/03/12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CA/BForum Baseline Requirements for issuance of SSL Certificates
V7.1	29/03/12	Lila Kee and Steve Roylance	Addition of support for NAESB and incorporation of the AlphaSSL product range
V7.2	07/06/12	Steve Roylance	Additional CA/BForum Baseline Requirements
V7.3	01/07/12	Steve Roylance	Final CA/BForum Baseline Requirements
V7.4	03/15/13	Giichi Ishii Lila Kee	Extended validity period of Personal Sign, Administrative updates/clarifications Modification to NAESB Certificates incorporating WEQ-012 v 3.0 updates
V7.5	03/31/13	Giichi Ishii	Statement of compliance to CA/Browser Forum Baseline Requirement, EPKI specification update
V7.6	03/07/14	Giichi Ishii Carolyn Oldenburg	Modified validity period for timestamping Certificate Added Certificate Data in the scope of archive Administrative updates/clarifications
V7.7	04/25/14	Giichi Ishii	Modified availability requirement and maximum process time for revocation Administrative update/clarifications
V7.8	02/09/14	Steve Roylance	Modifications to enhance the description of domain validation processes, highlighted by public review.

Detailed History of Changes

Changes in v.7.8 (Publication date: 21st August 2014) with respect to v.7.7

- Additional process clarification on SSL Domain Validation techniques used by GlobalSign

- Support for 4096 bit RSA and 521 bit ECC

Changes in v.7.7 (Publication date: June 4th 2014) with respect to v.7.6

- Extended maximum time to process revocation request
- Removed up time requirement for revocation status
- Changed company name of trademark owner
- Added Alpha SHA 256 CA

Changes in v.7.6 (Publication date: March 7, 2014) with respect to v.7.5

- Modified validity period for timestamping Certificate
- Added Certificate Data in the scope of archive
- Added provisions to ensure compliance with CA/Browser Forum Baseline Requirements
- Administrative updates/clarifications

Changes in v.7.5 (Publication date: 31th Mar 2013) with respect to v.7.4

- Added a statement of compliance to CA/Browser Forum Baseline Requirements
- Modified EPKI service specification

Changes in v.7.4 (Publication date: 15th Mar 2013) with respect to v.7.3

- Extended validity period of Personal Sign Product
- Administrative changes and clarifications
- Modification to NAESB certificates incorporating WEQ-012 v3.0 updates

Changes in v.7.3 (publication date: 1st July 2012) with respect to v.7.2

- Endorsement of additional CA/BForum Baseline Requirements – C name checking

Changes in v.7.2 (publication date: 7th June 2012) with respect to v.7.1

- Endorsement of additional CA/BForum Baseline Requirements

Changes in v.7.1 (publication date: 29th March 2012) with respect to v.7.0

- Support for NAESB Certificates
- Support for AlphaSSL Certificates

Changes in v.7.0 (publication date: 22nd March 2012) with respect to v.6.7

- Administrative changes and clarifications – Structural rewrite for RFC compliance and better understanding
- Removal of DocumentSign and introduction of Adobe CDS

Changes in v.6.7 (publication date: 18th May 2010) with respect to v.6.5

- Administrative changes and clarifications
- Removed Educational ServerSignSSL

Changes in v.6.6 (publication date: 27th January 2010) with respect to v.6.5

- Administrative changes supporting delivery of ObjectSign to Individuals. Rename ObjectSign to Code Signing

Changes in v.6.5 (publication date: 12th May 2009) with respect to v.6.4

- Administrative changes

Changes in v.6.4 (publication date: 11th February 2009) with respect to v.6.3

- Administrative changes
- Support of timestamping Certificate services.
- Support of Trusted Root TPM and DocumentSign

Changes in v.6.3 (publication date: 16th December 2008) with respect to v.6.2

- Administrative changes
- Support of enhanced validation and application processes – higher degree of automation

Changes in v.6.2 (publication date: 13th October 2008) with respect to v.6.1

- Administrative changes
- Clarification of Certificate Profiles and removal of Certificate Suspension.

Changes in v.6.1 (publication date: 20th May 2008) with respect to v.6.0

- Administrative changes
- SubjectAlternativeName and non-public domain support

Changes in v.6.0 (publication date: December 17th 2007) with respect to v.5.6

- Removal of the HyperSign product range
- The addition of role and department based PersonalSign Pro 2 Certificates
- The option for GlobalSign to generate Private Key pairs and CSRs on behalf of the Applicant
- The use of API functions for all products.
- Minor administrative changes to aid readability.

Changes in v.5.6 (publication date: June 25 2007) with respect to v.5.6

- Administrative changes
- Incorporation of modifications to support EV Guidelines at Issue 1.0

Changes in v.5.5 (publication date: June 19 2007) with respect to **v**.5.5

- Administrative changes
- Renamed some products

Changes in v.5.4 (publication date: March 30 2007) with respect to v.5.3

- Administrative changes

Changes in v.5.3 (publication date: Jan 26 2007) with respect to v.5.2
- Added GlobalSign DomainSSL product
- Added GlobalSign Root CA R2
- Adjusted Liability gap for OrganizationSSL and ExtendedSSL

Changes in v.5.2 (publication date: December 2006) with respect to v.5.1
- Added GlobalSign ExtendedSSL product
- Removed SureServer products, Renamed GlobalSign Educational ServerSign to GlobalSign Education GlobalSign OrganizationSSL.
- Administrative changes

Changes in v.5.1 (Publication Date: 13 March 2006) with respect to v.5.0
- Added GlobalSign Educational ServerSign product

Changes in v.5.0 (Publication Date: 10 July 2005) with respect to v.4.3.2
- Adaptation to the RFC 3647 format
- Separation of data protection policy, warranty policy and consumer policy.
- Updated references to GlobalSign Certificate Policy

Changes in v.4.3.2 (Publication Date: 8 April 2005) with respect to v.4.3.1
- Separated references to GlobalSign Qualified Certificates product

Changes in 4.3.1 (Publication Date: 10 October 2003) with respect to v.4.3
- Added SureServer product

Changes in 4.3 (Publication Date: 10 October 2003) with respect to v.4.2
- Section 1.4: Updated wording
- Section 4.3.6: Updated wording
- Section 5.13: Updated reference to logs retention period.
- Section 21.10: Updated wording
- Section 21.22: Updated wording
- Section 21.23: Updated wording

Changes in v.4.2 (Publication Date: 1 August 2003) with respect to v.4.1
- New Chapter 21 GlobalSign PersonalSign 3 Qualified certificates issued under Belgian Law of 9 July 2001 implementing the European Directive 1999/93/EC of the Council and the Parliament on a Community Framework on Electronic Signatures.
- Updated Chapter 10 GlobalSign Warranty Policy to include warranty requirements for product named GlobalSign PersonalSign 3 Qualified certificate.
- Updated Section 5.12 on records retention period for PersonalSign 3 Qualified certificate.
- Appropriate additions to the definitions list with regard to qualified certificates.
- Minor editorial updates to accommodate PersonalSign 3 Qualified in the Introduction.

Acknowledgments

This GlobalSign CA CPS conforms to:

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

This CPS conforms to the requirements of the following schemes:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria
- CA/BForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/B Forum Network and Certificate System Security Requirements

1.0 Introduction

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

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

This CPS addresses the technical, procedural and personnel policies and practices of GlobalSign CA during the complete lifecycle of Certificates issued by GlobalSign CA.

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

This CPS is final and binding between GlobalSign nv/sa, a company under public law, with registered office at Martelarenlaan 38, 3010 Leuven, VAT Registration Number BE 0459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (hereinafter referred to as "GlobalSign CA"), 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 toward those Relying Parties.

1.1 Overview

This CPS applies to the complete hierarchy of Certificates issued by GlobalSign CA. The purpose of this CPS is to present the GlobalSign CA practices and procedures in managing Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to GlobalSign CA's own and industry requirements pursuant to the standards set out above. Additionally, the Belgian Law of 9 July 2001 implementing the European Directive 1999/93/EC of the Council and the Parliament on a Community Framework on Electronic Signatures (the "Law") provides for the recognition of electronic signatures that are used for the purposes of authentication or non-repudiation. In this regard, GlobalSign CA operates within the scope of the applicable sections of the Law when delivering its services. This CPS aims to document the GlobalSign CA in delivery of certification services and management of the Certificate life cycle of any issued Subordinate CA, client, server and other purpose end entity Certificates. The Certificate types addressed in this CPS are the following:

PersonalSign 1/PersonalSign Demo	A personal Certificate of low assurance
PersonalSign 2	A personal Certificate of medium assurance
PersonalSign 2 Pro, Noble	A personal Certificate of medium assurance with reference to professional context

PersonalSign 2 Pro DepartmentSign	A machine, device, department, or role Certificate of medium assurance with reference to professional context
PersonalSign 3 Pro	A personal Certificate of high assurance with reference to professional context
PersonalSign Partners	A private Certification Authority created as a trust anchor issuing PersonalSign 2 Pro or PersonalSign 2 Pro DepartmentSign
Noble Energy	A machine, device, department, or role Certificate of medium assurance with reference to professional context
Internal SSL	A Certificate to authenticate internal servers, machines or routers
DomainSSL	A Certificate to authenticate web servers
AlphaSSL	A Certificate to authenticate web servers
OrganizationSSL & ICPEdu	A Certificate to authenticate web servers
ExtendedSSL	A Certificate to authenticate web servers *
GlobalSign Timestamping	A Certificate to authenticate time sources
GlobalSign CA for AATL	A personal Certificate of medium hardware assurance for use with Adobe AATL
Code Signing*	A Certificate to authenticate data objects
Extended Validation Code Signing*	A Certificate to authenticate data objects
North American Energy Standard Board (NAESB) Authorized CA Certificates	A personal, role, server or device Certificate of either rudimentary, basic, medium, or high assurance with reference to professional context authorized by an Authorized Certification Authority
PDF Signing for Adobe CDS**	A Certificate of medium hardware assurance chained to the Adobe Root CA which may have reference to a professional context.
PersonalSign for Adobe CDS	A Certificate issued to natural persons (individuals) without a professional context in affiliation with an organization for the purpose of signing Adobe PDF documents.
PersonalSign Pro for Adobe CDS	A personal digital ID issued with reference to professional context for the purpose of signing Adobe PDF documents
DepartmentSign for Adobe CDS	A role-based certificate with reference to professional context for the purpose of signing Adobe PDF documents
Trusted Root for Adobe CDS	A level 2 intermediate CA that enters the GlobalSign CA for Adobe hierarchy
Timestamping for Adobe CDS	A Certificate to authenticate time sources
Test Digital Certificate for Adobe CDS	A Certificate for test or demonstration purposes which does not require hardware Assurance

* These Certificates are issued and managed in accordance with the EV Guidelines and EV Code Signing Guidelines.
The remaining Certificate types shall be issued and managed in accordance with the Baseline Requirements if so indicated by the inclusion of CA/Browser Forum Policy OIDs as detailed in Section 1.2 below.
** These Certificates are issued and managed in accordance with the Adobe Systems Incorporated Certificate Policy at http://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf

GlobalSign CA Certificates:

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

This CPS identifies the roles, responsibilities and practices of all entities involved in the lifecycle, use, reliance upon and management of GlobalSign CA Certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including GlobalSign CA, GlobalSign

RA, Subscribers and Relying Parties. Certain provisions might also apply to other entities such as the certification service provider, application provider, etc.

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

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

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

Additionally, other relevant documents include:

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

A Subscriber or Relying Party of a GlobalSign Issuing CA Certificate must refer to this CPS in order to establish trust in a Certificate issued by GlobalSign CA as well as for information about the practices of GlobalSign CA. It is also essential to establish the trustworthiness of the entire Certificate chain of the hierarchy. This includes the Root CA Certificate as well as any operational Certificates. This can be established on the basis of the assertions within this CPS.

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

1.1.1 Certificate Naming

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

- GlobalSign Root CA – R1 with serial number 040000000001154b5ac394
- GlobalSign Root CA – R2 with serial number 0400000000010f8626e60d
- GlobalSign Root CA – R3 with serial number 04000000000121585308a2
- GlobalSign Root CA – R4 with serial number 2a38a41c960a04de42b228a50be8349802
- GlobalSign Root CA – R5 with serial number 605949e0262ebb55f90a778a71f94ad86c
- GlobalSign Primary SHA256 CA for Adobe serial number 35fbe4fadfe4b092276c319b99f8ceb3
- GlobalSign CA for Adobe with serial number 0100000000012872543bd4
- NAESB Issuing CA – SHA256 with serial number 5c76b72835bb871d2a81b65ea01ae1a832
- AlphaSSL G2 with serial number 0400000000012f4ee13702
- AlphaSSL G2 - SHA256 with serial number 040000000001444ef03631
- GlobalSign CA for AATL - SHA256 - G2 with serial number 040000000001444f0236b6
- Noble Energy CA SHA256 - G2 with serial number 63185ddb639a93798122fc17d0155349fc
- ICPEdu with serial number 57b09eef615610874491e92c5462f46196

GlobalSign CA actively promotes the inclusion of the five Root Certificates above (R1-R5) into hardware and software platforms that are capable of supporting Certificates and associated cryptographic services. Where possible, GlobalSign CA will seek to enter into a contractual agreement with platform providers to ensure effective Root Certificate life cycle management. However, GlobalSign CA also actively encourages platform providers at their own discretion to include GlobalSign CA Root Certificates without contractual obligation.

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

GlobalSign Trusted Platform Module Root CA with s/n 040000000000120190919AE [1]

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

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

GlobalSign CA expressly forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection.

1.2 Document Name and Identification

This document is the GlobalSign CA Certification Practice Statement.

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

1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy – SSL
1.3.6.1.4.1.4146.1.2	Extended Validation Certificates Policy – Code Signing
1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy
1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificates Policy - AlphaSSL
1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy
1.3.6.1.4.1.4146.1.30	Timestamping Certificates Policy
1.3.6.1.4.1.4146.1.31	Timestamping Certificates Policy - AATL
1.3.6.1.4.1.4146.1.40	Client Certificates Policy
1.3.6.1.4.1.4146.1.40.10	Client Certificates Policy (EPKI – Enterprise PKI)
1.3.6.1.4.1.4146.1.40.20	Client Certificates Policy (JCAN – Japan CA Network)
1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy
1.3.6.1.4.1.4146.1.60	CA Chaining Policy – Trusted Root
1.3.6.1.4.1.4146.1.60.1	CA Chaining Policy – Trusted Root compatible to CA/B Forum Baseline Requirements
1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90	Trusted Root TPM Policy
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy

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

2.16.840.1.114505.1.12.1.2	NAESB Rudimentary Assurance
2.16.840.1.114505.1.12.2.2	NAESB Basic Assurance
2.16.840.1.114505.1.12.3.2	NAESB Medium Assurance
2.16.840.1.114505.1.12.4.2	NAESB High Assurance

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

2.23.140.1.2.1	Domain Validation Certificates Policy
2.23.140.1.2.2	Organization Validation Certificates Policy

In addition to these identifiers, all Certificates that comply with the Adobe Systems Incorporated CP will include the following additional identifier:-

1.2.840.113583.1.1.5	Adobe Certified Document Services OID

[1] *Collectively Root R1 to R5 and the TPM Root are referred to as the GlobalSign CA Root Certificates*

1.3 PKI Participants

1.3.1 Certification Authorities

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

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

GlobalSign CA operates a secure facility in order to deliver CA services through an outsource agent. The GlobalSign CA outsource agent operates a service for GlobalSign CA on the basis of a service agreement. The scope of the outsourced services provided is Certificate issuance and revocation services. The GlobalSign CA outsource agent warrants designated services and service levels that meet those required by GlobalSign CA. The GlobalSign CA outsource agent carries out tasks associated with the administration of certain services and Certificates on behalf of GlobalSign CA. GlobalSign CA outsource agents are located in Belgium and France.

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

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

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

1.3.2 Registration Authorities

In addition to identifying and authenticating Applicants for Certificates, a Registration Authority (RA) may also initiate or pass along revocation requests for Certificates and requests for reissuance and renewal (sometimes referred to as re-key) of Certificates. GlobalSign CA may act as a Registration Authority for Certificates it issues in which case GlobalSign CA is responsible for:

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

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

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

Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of GlobalSign RAs or, as in the case of EPKI (Enterprise PKI) and MSSL (Managed SSL), are constrained by a pre-defined and validated GlobalSign Certificate Centre (GCC) configuration. These entities are also usually known as Enterprise RAs.

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

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

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

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

1.3.3 Subscribers

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

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

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

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

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

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

1.3.4 Relying Parties

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

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

1.3.5 Other Participants

Other participants include bridge CAs and CAs that cross certify Issuing CAs to provide trust among other PKI communities. For example, the GlobalSign CA Root R1 is cross certified by Microsoft to allow provision of 64

bit kernel mode drivers, naming GlobalSign CA as the Subject. The cross Certificate can be downloaded here:-

http://download.microsoft.com/download/2/4/E/24E730E6-C012-448F-92B6-78744D3B77E1/GlobalSign%20Root%20CA.zip

In Base64 format:-

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

1.4 Certificate Usage

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

1.4.1 Appropriate certificate usage

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

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

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

- **PersonalSign 2** non-repudiation of a transaction (medium level assurance)
- **PersonalSign 2/3 Pro** non-repudiation of the transaction by a party acting in an organizational context (medium level assurance)
- **Noble Energy** non-repudiation of the transaction by a party acting in an organizational context (medium level assurance)
- **CA for AATL** non repudiation of the transaction by a party acting in an organizational context (medium hardware level assurance)
- **PDF Signing** non-repudiation of the transaction by a party acting in an organizational context (medium hardware level assurance). *(It is not recommended that the Certificate be used for encryption due to the singularity of the Certificate and inability to provide key escrow services under the Adobe Certificate Policy.)*

- **PersonalSign 3 Pro** non-repudiation of the transaction by a party acting in an organizational context (high level assurance)

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

- **PersonalSign 1** authentication of the existence of an email address
- **PersonalSign 2** authentication of a natural person (medium level assurance) and the existence of an email address
- **PersonalSign 2 Pro** authentication of a natural person within an organizational context or a machine, device, department, or role within an organizational context (medium level assurance) and optionally the existence of an email address
- **Noble Energy** authentication of a natural person within an organizational context or a machine, device, department, or role within an organizational context (medium level assurance) and optionally the existence of an email address
- **CA for AATL** authentication of a natural person or a natural person within an organizational context or a role within an organizational context (medium level assurance) and optionally the existence of an email address
- **PersonalSign 3 Pro** authentication of a natural person within an organizational context (high level assurance)
- **NAESB Rudimentary** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB Basic** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB Medium** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB High** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1

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

- **DomainSSL** authentication of a remote Domain Name and webservice and encryption of the communication channel
- **AlphaSSL** authentication of a remote Domain Name and webservice and encryption of the communication channel
- **OrganizationSSL** authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel
- **ICPEdu** authentication of a remote Domain Name and associated organizational context and webservice and encryption of the communication channel
- **ExtendedSSL** authentication of a remote domain name and associated organizational context and webservice and encryption of the communication channel
- **Code Signing** authentication of a data object with a legal person or a Legal Entity
- **EV Code Signing** authentication of a data object with a legal person or a Legal Entity
- **Timestamping** authentication of a time and date related to a service within an organizational context
- **PersonalSign (All)** authentication of device or machine associated with an organization
- **NAESB Rudimentary** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB Basic** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB Medium** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB High** authentication as prescribed in NIST SP800-63 version 1.0.2 section 7.2.1

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

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

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

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

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

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

1.4.2 Prohibited Certificate usage

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorised. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the GlobalSign Warranty Policy.

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

Certificates issued under this CPS may not be used:-

- for any application requiring fail safe performance such as:

  - the operation of nuclear power facilities,
  - air traffic control systems,
  - aircraft navigation systems,
  - weapons control systems, and
  - any other system whose failure could lead to injury, death or environmental damage; or
- where prohibited by law.
- Certificates issued under the NAESB WEQ PKI shall never be used for performing any of the following functions:
  - Any transaction or data transfer that may result in imprisonment if compromised or falsified.
  - Any transaction or data transfer deemed illegal under federal law

1.4.2.1 Certificate extensions

Certificate extensions comply with X.509 v.3 standards.

- **PersonalSign 1 and Demo** Client authentication and secure email EKU
- **PersonalSign 2 / 2 Pro, Noble Energy** Client authentication and secure email EKU
- **PersonalSign 3 Pro** Client authentication and secure email EKU
- **NAESB** Can be used for protecting information of varying sensitivity including client authentication and secure email EKU, Client and server authentication EKU
- **GlobalSign CA for AATL** Client authentication and secure email EKU
- **OrganizationSSL, ICPEdu** Client and server authentication EKU
- **DomainSSL** Client and server authentication EKU
- **AlphaSSL** Client and server authentication EKU
- **ExtendedSSL** Client and server authentication EKU
- **Timestamping** Timestamping EKU
- **Code Signing and EV Code Signing** Code Signing EKU
- **PDF Signing** Adobe CDS Document Signing EKU
- **Trusted Root** All policies

1.4.2.2 Critical Extensions

GlobalSign CA also uses certain critical extensions in the Certificates it issues such as:

- A basic constraint in the key usage to show whether a Certificate is meant as a CA or not;
- To show the intended usage of the Certificate and the Public Key it contains in verifying signatures made by the matching Private Key;
- To show the number of levels that may be created below the hierarchy of the CA Certificate; and
- To constrain a Trusted Root CA Certificate to a customer's specific Domain Name Space(s).

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Policy Authority 2
GlobalSign NV
Martelarenlaan 38,
3010 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909

1.5.2 Contact Person

GlobalSign NV
attn. Legal Practices,
Martelarenlaan 38,
3010 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909

Email: legal@globalsign.com
URL: www.globalsign.com

1.5.3 Person Determining CPS Suitability for the Policy

Policy Authority 2 determines the suitability and applicability of the CP and the conformance of this CPS based on the results and recommendations received from a Qualified Auditor.

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

1.5.4 CPS Approval Procedures

Upon approval of a CPS update by the Policy Authority, the new CPS is published in the GlobalSign CA Repository at https://www.globalsign.com/repository.

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

1.6 Definitions and acronyms

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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).

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.

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): An HSM is 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.

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

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

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

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

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

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

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

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

AATL	Adobe Approved Trust List
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface

ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EIR	Electric Industry Registry
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
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
ICPEdu	A Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NAESB	North American Energy Standards Board
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax
WEQ	Wholesale Electric Quadrant

2.0 Publication and Repository Responsibilities

2.1 Repositories

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

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

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

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

2.2 Publication of Certificate Information

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

2.3 Time or Frequency of Publication

CA Certificates are published in a Repository via support pages as soon as possible after issuance. CRLs for end user Certificates are issued at least every 3 hours. CRLs for CA Certificates are issued at least every 6 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after being digitally signed by the CPS Policy Authority using an Adobe CDS PDF signing Certificate with appropriate time stamp.

2.4 Access control on repositories

While GlobalSign CA generally provides access to its Repository and its policies (e.g. CP, CPS) free of charge, it might charge for services such as the publication of status information on third party databases and private directories.

GlobalSign CA ensures the integrity and authenticity of its public documentation through the use of Digital Signatures applied to PDF documents.

3.0 Identification and Authentication

GlobalSign CA acts as an RA that verifies and authenticates the identity and/or other attributes of an Applicant.

Applicants are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others. GlobalSign CA 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 CA reserves the right, without liability to any Applicant, to reject an application because of such a dispute.

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

3.1 Naming

3.1.1 Types of Names

GlobalSign CA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading. However, some Certificates such as Unified Communications SSL Certificates may include subject alternative name extensions that are not publicly routable such as .local or private IP addresses that are defined by RFC 1918. GlobalSign CA may also include RFC2460 (IP version 6) or RFC791 (IP version 4) addresses.

Non wildcard SSL Certificates and Unified Communications Certificates are issued with a Fully Qualified Domain Name (FQDN) name or IP address.

Wildcard SSL Certificates include a wildcard asterisk character. Before issuing a Certificate with a wildcard character (*) GlobalSign CA follows best practices to determine if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”. (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation.) and if it does, it will reject the request as the Domain Namespace must be owned or controlled by the Subscriber, e.g. *.globalsign.com.

In the case of SSL Certificates, whilst the FQDN or authenticated Domain Name is placed in the Common Name (CN) attribute of the Subject field, it may also be duplicated into the Subject Alternative Name extension along with a www version of the DNS-ID. Subject Alternative Names are marked non critical in line with RFC5280.

3.1.2 Need for Names to be Meaningful

Where possible, GlobalSign CA uses distinguished names to identify both the Subject and the Issuing CA of a Certificate. In cases where a GlobalSign CA product allows the use of role or departmental name additional unique elements may be added to the DN within the OU field to allow differentiation between Certificates with common DN elements by Relying Parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

GlobalSign CAs may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and where possible name space uniqueness is preserved. GlobalSign CA 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. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

GlobalSign CA enforces the uniqueness of each Subject name in a Certificate as follows.

- **PersonalSign1 Certificates** A unique email address only.
- **PersonalSign Certificates** A unique email address (if to be included in the Certificate subjectDN) and the name of an individual along with the name of the Country which issued the passport or equivalent credential the individual provides to prove their identity to GlobalSign CA .
- **PersonalSign Pro Certificates** A unique email address (if to be included in the Certificate subjectDN) coupled with an organization’s name and address plus either the name of and individual or a department associated with the organization.

• **Noble Energy Certificates**	A unique email address (if to be included in the Certificate subjectDN) coupled with an organization's name and address plus either the name of an individual or a department associated with the organization.
• **Code Signing Certificates**	A unique organization name and address or a unique individual name and address with an optional email address.
• **SSL Certificates**	A Domain Name within the Common Name attribute as approved as unique by ICANN.
• **Timestamping Certificates**	A unique organization name and address with an optional email address.
• **CA for AATL Certificates**	Most commonly, a unique email address coupled with an organization's name and address plus either the name of an individual or a department associated with the organization. Less frequently, a unique email address and the name of an individual along with the name of the Country which issued the passport or equivalent credential the individual provides to prove their identity to GlobalSign.
• **NAESB Rudimentary**	A unique email address only.
• **NAESB Basic, Medium, and High**	A unique email address coupled with an organization's name and address plus either the name of an individual or a department associated with the organization.
• **PDF Signing Certificates**	Most commonly, a unique email address coupled with an organization's name and address plus either the name of an individual or a department associated with the organization. Less frequently, a unique email address and the name of an Individual along with the name of the Country which issued the passport or equivalent credential the individual provides to prove their identity to GlobalSign.
• **Trusted Root**	Follows the Baseline Requirements for Subject naming

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

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

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

3.2.1 Method to Prove Possession of Private Key

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

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

3.2.2 Authentication of Organization Identity

GlobalSign CA maintains internal policies and procedures which are reviewed regularly in order to comply with the requirements of the various root programs that GlobalSign CA is a member of, as well as the Baseline Requirements, the EV Guidelines and EV Code Signing Guidelines. These policy and procedure documents are under the control of Policy Authority 6 (subordinate to the main Policy Authority in section 1.5.1) fulfilling the criteria of Principle 6 of the WebTrust 2.0. The method by which GlobalSign verifies the organization identity is generally consistent across all product types, however alternative methods, in line with accepted alternatives, may be used where authentication is not possible through the more commonly used QGIS method highlighted below.

For all Certificates that include an organization identity, Applicants are required to indicate the organization's name and registered or trading address. For all Certificates, the legal existence, legal name, assumed name, legal form and requested address of the organization are verified using one of the following:-

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

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

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

3.2.2.1 Local Registration Authority Authentication

For EPKI and MSSL accounts, GlobalSign CA 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. *(Whilst LRA's are able to authenticate individuals under contract, all domains to be authenticated will have previously been verified by GlobalSign CA).*

3.2.2.2 Role Based Certificate Authentication (DepartmentSign)

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

3.2.3.1 Class 1 (Personal Sign 1 & PersonalSign 1 Demo Certificates)

The Applicant is required to demonstrate control of the email address to which the Certificate relates. GlobalSign CA does not authenticate additional information provided by the Applicant during the GCC signup and enrolment process.

3.2.3.2 Class 2 (PersonalSign2, SSL, Code Signing, PDF Signing for Adobe CDS & AATL for Individuals)

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

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

GlobalSign CA also authenticates the Applicant's identity through one of the following methods:

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

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

3.2.3.3 Class 3 (PersonalSign3 Pro Certificates)

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

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

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. This is mandated within the business process for PersonalSign 3 Pro).

GlobalSign CA authenticates the Applicant's authority to represent the organization wishing to be named as the Subject in the Certificate by one of the following methods:

- Performing a telephone challenge/response to the Applicant's organization using a telephone number from a reliable source; or
- Performing a postal challenge to the Applicant's organization using an address obtained from a reliable source.

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

3.2.3.4 Local Registration Authority Authentication

For EPKI and MSSL accounts, which allow the concept of a Local Registration Authority, GlobalSign CA sets authenticated organizational details in the form of a profile. Suitably authenticated account administrators acting in the capacity of a Local Registration Authority are contractually obligated to authenticate individuals affiliated with the organization.

3.2.3.5 North American Energy Standards Board (NAESB) Certificates

For NAESB Certificate requests, authenticity of organization identity requests for Certificates in the name of an affiliated organization shall include the organization name, address, and documentation of the existence of the organization. GlobalSign or the RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization. End entities shall be obligated to register their legal business identification and secure an "Entity Code" that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that end entity.

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

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

Registration of Identity Proofing Requirements shall use the following mappings:

NIST Assurance Level	NAESB Assurance Level
Level 1	Rudimentary
Level 2	Basic
Level 3	Medium
Level 4	High

GlobalSign CA, or its designated RA in the case of EPKI, shall verify all of the identification information

supplied by the Applicant in compliance with the authentication requirements defined by NIST SP800-63 version 1.0.2 section *7.2.1* found at http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

3.2.4 Non-Verified Subscriber Information

GlobalSign CA validates all information to be included within the Subject DN of a Certificate except where highlighted within this section of the CPS. GlobalSign CA uses the Subject: organizationalUnitName as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices.

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

- For all Certificate types where GlobalSign CA cannot explicitly verify the identity, e.g. a generic term such as "Marketing", then GlobalSign CA omits any disclaimer that this item is classified as non-verified Subscriber information as described herein. For OV SSL/TLS Certificates only, GlobalSign CA relies upon information provided by the Applicant to be included within the subjectAlternativeName such as internal or non-public DNS names, hostnames and RFC 1918 IP addresses. The Baseline Requirements define the time frame for an industry wide deadline at which time these objects may no longer be included within Certificates. Until such time these items are classified as non-verified Subscriber information as ownership cannot reasonably be validated.

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

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

3.2.5 Validation of Authority

• **PersonalSign1 Certificates**	Verification that the Applicant has control over the email address to be listed within the Certificate through a challenge response mechanism.
• **PersonalSign2 Certificates**	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included.
• **Noble Energy Certificates**	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included.
• **NAESB Certificates**	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included (see Section 3.2.3.5.)
• **PersonalSign3 Certificates**	Verification through a reliable means of communication with the organization that the Applicant represents the organization. Personal appearance is mandatory before a suitable Registration Authority to validate the personal credentials of the Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate.
• **Code Signing Certificates**	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address that may be optionally listed within the Certificate.
• **EV Code Signing Certificates**	Verifying the authority of the contract signer and Certificate approver in accordance with the EV Guidelines and EV Code Signing Guidelines.
• **DV/AlphaSSL Certificates**	Validation of the ownership or control of the domain name by a suitable challenge response mechanism. Either:-

	▪ Using GlobalSign's OneClickSSL protocol whereby the Applicant is required to demonstrate control of a domain by installing a non-publicly trusted test Certificate of GlobalSign CA's design, ▪ By uploading specific metadata to a defined page on the domain, ▪ By direct confirmation with the contact listed with the Domain Name Registrar, ▪ Successfully replying to a challenge response email sent to one or more of the following email addresses: • webmaster@domain.com, postmaster@domain, admin@domain.com administrator@domain.com, hostmaster@domain, or • any address listed as a contact field of the WHOIS record. ▪ If the Country code is included within the DN then GlobalSign validates the Country based on the geo-location of the IP address obtained by a DNS query.
• **OV SSL & ICPEdu Certificates**	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has ownership or control of the domain name by either a challenge response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS.
• **EV SSL Certificates**	Verifying the authority of the contract signer and Certificate approver in accordance with the EV Guidelines.
• **Time Stamping Certificates**	Verification through a reliable means of communication with the organization's Applicant.
• **CA for AATL Certificates**	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address to be listed within the Certificate.
• **PDF Signing for Adobe CDS Certificates**	Verification through a reliable means of communication with the organization or individual Applicant.
• **Trusted Root**	Verification through a reliable means of communication with the organization's Applicant.

3.2.6 Criteria for Interoperation

Not applicable

3.2.7 Authentication of Domain Name

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

- Using GlobalSign's OneClickSSL protocol whereby the Applicant is required to demonstrate control of a Domain Name by installing a non publicly trusted test Certificate of GlobalSign CA's specification. GlobalSign CA then makes a connection to the test Certificate over https to verify the use of the Private/Public Key Pair on the domain(s) being authenticated. Publicly trusted Certificates will be delivered to the Applicant based on the same Public/Private Key Pair;
- By uploading specific metadata to a defined page on the domain;
- By uploading specific metadata to the DNS text record of the domain;
- By direct confirmation with the contact listed by the Domain Name Registrar in the WHOIS record or provided to GlobalSign CA by the Domain Name Registrar directly;
- By successfully replying to a challenge response email sent to one or more of the following email addresses:
    - webmaster@domain.com, postmaster@domain, admin@domain.com, administrator@domain.com, hostmaster@domain, or
    - any email address listed as a contact field of the WHOIS record, or
    - any address previously used for the successful validation of the control of the domain subject to the re-verification requirements of Section 3.3.1; or
- By receiving a reliable communication from the Domain Name Registrar stating that the Registrant gives the Applicant permission to use the Domain Name.

To reduce the risk of compromise of the WHOIS information, GlobalSign only uses the WHOIS records linked to on the IANA root database and the WHOIS records provided by ICANN approved registrars.

The following information on the WHOIS records can be used:

- Name;
- Telephone number;
- Fax number;
- Address;
- Email address.

This information is taken from the following fields (where applicable):

- Registrar;
- Registrant, holder, domain owner or similar;
- Technical contact;
- Administrative contact.

3.3 Identification and Authentication for Re-key Requests

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

3.3.1 Identification and Authentication for Routine Re-key

- **PersonalSign1 Certificates** Username and password required with re-verification every 9 years.
- **PersonalSign2 Certificates** Username and password required with re-verification every 9 years or client authentication with a current unexpired and unrevoked Certificate.
- **Noble Energy Certificates** Username and password required with re-verification every 9 years or client authentication with a current unexpired and unrevoked Certificate.
- **PersonalSign3 Certificates** Username and password required with re-verification every 6 years.
- **Code Signing Certificates** Username and password required with re-verification every 6 years.
- **EV Code Signing Certificates** Username and password required with re-verification as indicated by the EV Guidelines and/or EV Code Signing Guidelines.
- **DV SSL Certificates** Username and password required with re-verification every 5 years.
- **OV SSL & ICPEdu Certificates** Username and password required with re-verification every 5 years.
- **EV SSL Certificates** Username and password required with re-verification as indicated by the EV Guidelines.
- **Timestamping Certificates** Not supported.
- **CA for AATL Certificates** Username and password required with re-verification every 6 years.
- **PDF Signing for Adobe CDS Certificates** Not supported
- **Trusted Root** Not supported.
- **AlphaSSL** Not supported.
- **NAESB Certificates** Subscribers of Authorized Certification Authorities shall identify themselves for the purpose of reissuing as required in the table below.

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

Medium	Identity may be established through use of current Private Key, except that identity shall be established through initial registration process at least once every three years from the time of initial registration.
High	Identity may be established through use of current Private Key, except that identity shall be established through initial registration process at least annually.

3.3.2 Identification and Authentication for Reissuance after Revocation

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

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

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

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

3.3.4 Identification and Authentication for Re-key After Revocation

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

3.4 Identification and Authentication for Revocation Request

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

- **PersonalSign1 Certificates** Username and password or out of band.
- **PersonalSign2 & Pro Certificates** Username and password or out of band.
- **Noble Energy** Username and password or out of band.
- **NAESB Certificates** Username and password or out of band.
- **PersonalSign3 Pro Certificates** Username and password or out of band.
- **Code Signing Certificates** Username and password or out of band.
- **EV Code Signing Certificates** As indicated by the EV Guidelines.
- **DV SSL Certificates** Username and password or out of band or proof of possession of domain control using OneClickSSL.
- **AlphaSSL Certificates** Out of band or proof of possession of domain control using OneClickSSL.
- **OV SSL & ICPEdu Certificates** Username and password or out of band.
- **EV SSL Certificates** Username and password or out of band.
- **Timestamping Certificates** Out of band process.
- **CA for AATL Certificates** Username and password or out of band.
- **PDF Signing for Adobe CDS Certificates** Username and password or out of band.
- **Trusted Root** Out of band process.

GlobalSign CA may also perform revocation on behalf of Subscribers in accordance with the requirements of its Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non-payment of applicable fees.

4.0 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

GlobalSign CA maintains its own blacklists of individuals from whom and entities from which it will not accept Certificate applications. In addition, other external sources such as government denied lists or internationally

recognized denied persons lists which are applicable to the jurisdictions in which GlobalSign CA operates are used to screen out unwanted Applicants.

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

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

Applications are accepted via one of four methods:-

- **On-line** Via a web interface over an https session. An Applicant must submit an application via a secure ordering process according to a procedure maintained by GlobalSign CA. The majority of direct customers use this method, known as GCC. It requires users to maintain an account with suitably strong username and password for ongoing maintenance of the lifecycle of the Certificate. The account may be classified as MSSL, EPKI, retail, partner or reseller.
- **API** Resellers, partners and large enterprises who are Applicants submit an appropriately formatted Certificate Request via an approved API (Application Programming Interface) to GlobalSign CA with a suitably strong username and password. The source IP address of the Applicant may be required by GlobalSign CA if no other constraints are applicable. The account may be classified as API or SAPI (Simple API).
- **OneClickSSL** Applicants using one of the approved OneClickSSL plug-in tools may submit a request without an account. In this case the Domain Name is used for the initial and future lifecycle management tasks assuming that sufficient Domain Name control has been verified within the applicable session.
- **Manual** Applicants wishing to enter the Trusted Root program, issue timestamping certificates, or those requiring a greater number of SubjectAlternativeName entries in a Certificate than the GCC system supports are required to submit applications both electronically in the form of an email and out of band such that the request can be sufficiently authenticated and verified.

4.1.2 Enrollment Process and Responsibilities

GlobalSign CA 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 CA and any GlobalSign RA to successfully perform the required verification. GlobalSign CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process in compliance with the GlobalSign CA Privacy Policy.

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

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

GlobalSign CA shall reject requests for Certificates where validation of all items cannot successfully be completed. GlobalSign CA may also reject requests based on potential brand damage to GlobalSign CA in

accepting the request. GlobalSign CA may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement.

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

Assuming all validation steps can be completed successfully following the procedures within this CPS then GlobalSign CA shall approve the Certificate Request.

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

4.2.3 Time to Process Certificate Applications

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

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

The following approximations are given for processing and issuance.

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

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

GlobalSign CA 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 work flow of the Certificate requested.

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

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

GlobalSign CA publishes the Certificate by delivering it to the Subscriber. In addition, for enterprise customers GlobalSign CA may publish the Certificate into a directory such as LDAP.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs, local RA or partners/resellers or GlobalSign CA 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 CA provides a suitable Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate. Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CPS GlobalSign CA provides the conditions under which Certificates may be relied upon by Relying Parties including the appropriate Certificate services available to verify Certificate validity such as CRL and/or OCSP. GlobalSign CA provides a Relying Party agreement to Subscribers, the content of which should be presented to the Relying Party prior to reliance upon a Certificate from GlobalSign CA. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made.

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

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is defined as the production of a new Certificate that has the same fields defined as a previously issued Certificate and the same public key but contains a new 'Not After' date.

GlobalSign CA supports renewal for the following products and services:-

- **PersonalSign1 Certificates** Renewal supported as a re-key via GCC
- **PersonalSign2 Certificates** Renewal supported as a re-key via GCC
- **PersonalSign2 Pro Certificates** Renewal supported as a re-key via GCC
- **Nobel Energy Certificates** Renewal supported as a re-key via GCC
- **PersonalSign3 Pro Certificates** Renewal supported as a re-key via GCC
- **Code Signing Certificates** Renewal supported as a re-key via GCC
- **EV Code Signing Certificates** Renewal supported as a re-key via GCC
- **DV SSL Certificates** Renewal supported as a re-key via GCC
- **AlphaSSL Certificates** Renewal supported as a re-key via GCC
- **OV SSL & ICPEdu Certificates** Renewal supported as a re-key via GCC
- **EV SSL Certificates** Renewal supported as a re-key via GCC
- **Timestamping Certificates** Renewal supported via manual processes
- **NAESB Certificates** Renewal supported as a re-key via GCC
- **CA for AATL Certificates** Renewal supported as a re-key via GCC
- **PDF Signing for Adobe CDS Certificates (all)** Renewal supported as a re-key via GCC
- **Managed SSL (MSSL)** Functions are built in to the product
- **Enterprise PKI (EPKI)** Functions are built in to the product

- **Trusted Root** Renewal supported via manual processes

. GlobalSign CA may renew a Certificate so long as:-

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

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

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

GlobalSign CA may request additional information before processing a renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Certificate re-key is defined as the production of a new Certificate that has the same details as a previously issued Certificate but has a new Public Key and a new 'Not After' date.

If a Certificate is re-keyed prior to the 'Not After' date expiring and given the same 'Not After' date refers to this as reissue.

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

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

. GlobalSign CA may re-key a Certificate as long as:-

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

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

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-Keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

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

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

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a CRL. The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding a serial number allows Relying Parties to establish that the lifecycle of a Certificate has ended. GlobalSign CA may remove serial numbers when revoked Certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation GlobalSign CA will verify the authenticity of the revocation request. Revocation of a Subscriber Certificate shall be performed within twenty-four (24) hours under the following circumstances:-

- The Subscriber requests in writing to the GlobalSign entity which provided the Certificate that they wish to revoke the Certificate;
- The Subscriber notifies GlobalSign CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- GlobalSign CA obtains reasonable evidence that the Subscriber's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- GlobalSign CA receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;
- GlobalSign CA is made aware of any circumstance indicating that used of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- GlobalSign CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- GlobalSign CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
- GlobalSign CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements or GlobalSign's CP or this CPS;
- If GlobalSign CA determines that any of the information appearing in the Certificate is not accurate or is misleading;
- GlobalSign CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- GlobalSign CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless GlobalSign CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- GlobalSign CA is made aware of a possible Compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
- Revocation is required by GlobalSign CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);

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

- The Subscriber or organization administrator requests revocation of the Certificate through a GCC account which controls the lifecycle of the Certificate;
- The Subscriber requests revocation of the Certificate via a OneClickSSL revocation workflow process;
- The Subscriber requests revocation through an authenticated request to GlobalSign CA's support team or GlobalSign CA's Registration Authority;
- GlobalSign CA receives notice or otherwise become aware that the Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GlobalSign CA's jurisdiction of operation; and
- GlobalSign determines the continued use of the Certificate is harmful to the business of GlobalSign CA and Relying Parties.

When considering whether Certificate usage is harmful to GlobalSign's brand, GlobalSign CA considers, among other things, the following:

- The nature and number of complaints received;
- The identity of the complainant(s);
- Relevant legislation in force; and
- Responses to the alleged harmful use from the Subscriber.

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

- The Subordinate CA requests in writing to the GlobalSign entity which provided the Subordinate CA Certificate or the authority detailed in Section 1.5.2 of this CPS, that GlobalSign CA revoke the Certificate;
- The Subscriber notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains reasonable evidence that the Subordinate CA's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that the Subordinate CA has not complied with the Baseline Requirements or the applicable CP or this CPS;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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

4.9.2 Who Can Request Revocation

GlobalSign CA and RAs shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the Certificate. GlobalSign CA may also at its own discretion revoke Certificates including Certificates that are issued to other cross signed CAs.

4.9.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, GlobalSign CA provides automated mechanisms for requesting and authenticating revocation requests. The primary method is through the GCC account used to issue the Certificate that is requested to be revoked. Alternative out of band methods may be used, such as receipt of a fax/letter/phone call, the origins of which must be authenticated using shared secrets from the GCC account. Alternatively, where GCC accounts are not provided, methods may be used which rely on a demonstration of control of one or more elements of the Subject DN of the Certificate. For SSL/TLS, this could involve using the OneClickSSL protocol to demonstrate control/ownership of the dNSDomainName. For SMIME Certificates it could include demonstration of control of the email address.
GlobalSign CA 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.
Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

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

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

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

4.9.6 Revocation Checking Requirements for Relying Parties

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

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

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

4.9.7 CRL Issuance Frequency

GlobalSign CA meets the requirements of the Baseline Requirements and the EV Guidelines (if applicable) with respect to CRL issuance frequency. GlobalSign's Root CAs and offline CAs publish a CRL every 6 months. GlobalSign CAs G2 (Generation 2) and G2-SHA256 (Generation 2 supporting SHA256) online CAs have CRLs, which are published every 3 hours and are valid for 1 week. GlobalSign previous CAs which no longer issue Certificates but continue to issue CRLs may vary with the CRL validity between 1 week and 1 month.

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

In the case of Code Signing Certificates that have been revoked due to key Compromise or issued to unauthorized persons revoked Certificates will be maintained on the CRL for at least 20 years following revocation.

GlobalSign CA requires OCSP requests to contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation information otherwise all warranties becomes void.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

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

4.9.13 Circumstances for Suspension

GlobalSign CA does not support suspension.

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

GlobalSign CA provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. These services are presented to Relying Parties within the Certificate and may refer to any of the following URLs

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

4.10.2 Service Availability

GlobalSign CA maintains 24x7 availability of Certificate status services with appropriate additional content distribution network cloud-based mechanisms to aid service availability of cacheable results.

4.10.3 Operational Features

No stipulation

4.10.4 End of Subscription

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

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

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

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

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

5.1.1 Site Location and Construction

GlobalSign CA ensures that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. These are physically protected from unauthorized access, damage and interference and the protections provided are commensurate with the identified risks in risk analysis plans.

5.1.2 Physical Access

GlobalSign CA ensures that the facilities used for Certificate lifecycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee will always accompany any unauthorized person entering a physically secured area. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises are shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

GlobalSign CA ensures that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

GlobalSign CA ensures that the CA systems are protected from water exposure.

5.1.5 Fire Prevention and Protection

GlobalSign CA ensures that the CA system is protected with a fire suppression system.

5.1.6 Media Storage

GlobalSign CA ensures that any media used is securely handled to protect it from damage, theft and unauthorized access. Media management procedures ensure (i) media is protected against obsolescence and deterioration of the media within a defined period of time and (ii) records are retained. All media is handled securely in accordance with requirements of the information asset classification scheme and media containing sensitive data is securely disposed of when no longer required.

5.1.7 Waste Disposal

GlobalSign CA ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

GlobalSign CA ensures that a full system backup of the Certificate issuance system is sufficient to recover from system failures and is made once per week. Back-up copies of essential business information and software are also taken once per week. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of business continuity plans. At least one full backup copy is stored at an offsite location (at a location separate from the Certificate issuance equipment). Backups are stored at a site with physical and procedural controls commensurate to that of the operational facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

Trusted roles include but are not limited to the following:

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

5.2.2 Number of Persons Required per Task

GlobalSign CA requires at least two people per task. The goal is to guarantee the trust for all CA services (Key Pair generation, Certificate generation, and revocation) so that any malicious activity would require collusion.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, GlobalSign CA 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 CA enforces role separation either by the CA equipment or procedurally or by both means. Individual CA personnel are specifically assigned to the roles defined in Section 5.2.1 above. It is not permitted for any one person to serve in the following roles at the same time:

- Security officer and System Engineer or Operator;
- Auditor and Security Officer or Operator or Administrator or System Engineer;
- System Engineer and Operator or Administrator.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

GlobalSign CA employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. GlobalSign CA 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 CA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. GlobalSign CA personnel are formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

5.3.2 Background Check Procedures

All GlobalSign CA personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the CA operations. GlobalSign CA does not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence if such conviction affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed and results analysed, provided such checks are permitted by the jurisdiction in which the person will be employed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

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

5.3.3 Training Requirements

GlobalSign CA ensures that all personnel performing duties with respect to the operation of the CA receive comprehensive training in:

- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

GlobalSign CA and RA personnel are retrained when changes occur in GlobalSign CA or RA systems. Refresher training is conducted as required and GlobalSign CA shall review refresher training requirements at least once per year.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Contractor personnel employed for GlobalSign CA 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 CA makes available to its personnel this CPS, any corresponding CP and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.
Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

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

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

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

Audit log records are held for a period of time as appropriate to provide necessary legal evidence in accordance with any applicable legislation. Records may be required at least as long as any transaction relying on a Valid Certificate can be questioned.

5.4.4 Protection of Audit Log

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

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

The records of events are date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

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

5.5 Records Archival

5.5.1 Types of Records Archived

GlobalSign CAs and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. At a minimum, the following data is archived:

GlobalSign CA key life cycle management events, including:-

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

GlobalSign CA issuance system management events including:-

- System start-up and shutdown actions;
- Attempts to create, remove, or set passwords or change the system; and
- Changes to Issuing CA Private Keys.

GlobalSign CA and Subscriber Certificate life cycle management events, including:-

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

Security events, including:-

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

Documentation and Auditing:-

- Audit documentation including all work related communications to or from GlobalSign CA and compliance auditors;
- Certificate Policy and previous versions;
- Certification Practice Statement and previous versions; and
- Contractual agreements between Subscribers and GlobalSign CA

Timestamping:-

- Clock synchronisation.

Miscellaneous:-

- Other data or applications sufficient to verify archive contents;
- Equipment failure;
- UPS failure or electrical power outages; and
- Violations of the CP or this CPS.

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 10 years, however a GlobalSign LRA (for EPKI) may retain records for a shorter period of time.

5.5.3 Protection of Archive

The archives are created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Timestamping of Records

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

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of GlobalSign CA archive information is checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.
Only authorised GlobalSign CA 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 CA may periodically change over key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may also be modified and Certificate profiles may be altered to adhere to best practices. Private Keys used to sign previous Subscriber Certificates are maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

GlobalSign CA establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or Compromise the GlobalSign CA services. GlobalSign CA carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary *(threat evolution, vulnerability evolution, etc).* This business continuity is included in the scope of the audit process as described in Section 8 to validate which operations should be first restored after a disaster and the recovery plan.
GlobalSign CA personnel that serve in a trusted role and operational role are specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.

If GlobalSign CA detects a potential hacking attempt or another form of Compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, GlobalSign CA assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether

only some Certificates need to be revoked, and/or whether a CA hierarchy needs to be declared as Compromised. The CA disaster recovery plan highlights which services should be maintained *(for example, revocation and Certificate status information).*

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

If any equipment is damaged or rendered inoperative but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to GlobalSign CA'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 CA, after investigation of the problem, shall decide if the GlobalSign CA Certificate should be revoked. If so, then:-
    - All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and
    - A new GlobalSign CA Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.

5.7.4 Business Continuity Capabilities After a Disaster

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

5.8 CA or RA Termination

In the event of termination of a GlobalSign CA or RA, GlobalSign CA provides notice to all customers prior to the termination and:

- Stops delivering Certificates according to and referring to this CPS;
- Archives all audit logs and other records prior to termination;
- Destroys all Private Keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as another GlobalSign CA that delivers identical services;
- Uses secure means to notify customers and Application Software Suppliers to delete all trust anchors.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

GlobalSign CA generates all issuing Key Pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. External witnesses (Ideally an independent auditor who normally performs audits on a regular basis) is present and the ceremony, as a whole, is videotaped/recorded. GlobalSign CA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

GlobalSign CAs that create Private Keys on behalf of Subscribers (AutoCSR) do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. For SSL/TLS Certificates, this is achieved through the use of PCKS#12 (.pfx) files containing Private Keys and Certificates encrypted by a sixteen (16) digit password. The first eight (8) digits are system generated and provided to the Subscriber during the enrollment process and the Subscriber decides the remaining eight (8). For SMIME certificates, this is again achieved through the use of PCKS#12 (.pfx) files containing Private Keys and Certificates encrypted by an eight (8) digit Subscriber-selected password.

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

6.1.3 Public Key Delivery to Certificate GlobalSign CA

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

6.1.4 CA Public Key Delivery to Relying Parties

GlobalSign CA ensures that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks. The Certificates highlighted in Section 1.1 are available for download via https:// URLs and this CPS document is protected by a Certificate issued under the Adobe CDS program, protecting the integrity and authenticity of content (i.e. the serial numbers highlighted in Section 1.1). Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys into their root stores and operating systems. Issuing CA Public Keys are delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by GlobalSign CA and referenced within the profile of the issued Certificate through AIA (Authority Information Access).

6.1.5 Key Sizes

GlobalSign CA follows NIST Special Publication 800-133 (2012) - Recommendation for Cryptographic Key Generation - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Issuing CAs and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root program, outside of the direct control of GlobalSign CA are contractually obligated to use the same best practices.
GlobalSign CA selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the Baseline Requirements and EV Guidelines:-

RSA

- 2048 bit RSA key with Secure Hash Algorithm 1 (SHA-1)
- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)
- 4096 bit RSA key with Secure Hash Algorithm 2 (SHA-384)

ECC

- 256 bit ECDSA key with Secure Hash Algorithm 2 (SHA-256)
- 384 bit ECDSA key with Secure Hash Algorithm 2 (SHA-384)
- 521 bit ECDSA key with Secure Hash Algorithm 2 (SHA-512)

6.1.6 Public Key Parameters Generation and Quality Checking

GlobalSign CA 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 shall be tested for and rejected at the point of submission.

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

GlobalSign CA 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).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

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

GlobalSign CA activates Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code). The Root Certificate Private Key is always protected through 3 of 5.

6.2.3 Private Key Escrow

GlobalSign CA does not escrow Private Keys for any reason.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

GlobalSign CA does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

GlobalSign CA 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 CA 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 CA destroys all associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

GlobalSign CA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

Type	Private Key Usage	Max Validity Period
• **Root Certificates**[2]	20 years	30 years
• **TPM Root Certificates**	30 years	40 years
• **Issuing CA**	11 years	15 years
• **PersonalSign Certificates**	No stipulation	5 years
• **Nobel Energy Certificates**	No stipulation	5 years
• **Code Signing Certificates**	No stipulation	3 years
• **EV Code Signing Certificates**	No stipulation	39 months
• **DV SSL Certificates**	No stipulation	5 years
• **AlphaSSL Certificates**	No stipulation	5 years
• **OV SSL & ICPEdu Certificates**	No stipulation	5 years
• **EV SSL Certificates**	No stipulation	27 months
• **Timestamping Certificates**	11 years	133 months
• **CA for AATL Certificates**	No stipulation	181 months
• **PDF Signing for Adobe CDS Certificates**	No stipulation	5 years
• **Trusted Root**	No stipulation	10 years
• **NAESB Certificates**	2 years	2 years

GlobalSign CA complies with the Baseline Requirements with respect to the maximum Validity Period. In some cases, the maximum validity period may not be realized by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for

[2] *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.*

reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

Effective April 1, 2015, in no event shall GlobalSign issue an SSL/TLS Certificate with a validity period greater than 39 months whether as initial issue, re-key, reissue or otherwise.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of GlobalSign CA 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.

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

- Require authenticated logins for trusted role;
- Provide discretionary access control;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide domain isolation for process; and
- Provide self-protection for the operating system.

When GlobalSign CA PKI equipment is hosted on an evaluated platform in support of computer security assurance requirements then the system (hardware, software, operating system), when possible, operates in an elevated configuration. At a minimum, such platforms use the same version of the computer operating system as that which received the evaluation rating. The computer systems are configured with minimum of the required accounts, network services, and no remote login.

6.5.2 Computer Security Rating

All the GlobalSign CA PKI component software is compliant with the requirements of the protection profile from a suitable entity.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for GlobalSign CA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;

- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are installed on the equipment and are obtained from sources authorized by local policy. GlobalSign CA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

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

6.6.3 Lifecycle Security Controls

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

6.7 Network Security Controls

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

6.8 Time Stamping

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

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

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

6.8.1 PDF Signing Time Stamping Services

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

6.8.2 Code Signing and EV Code Signing Time Stamping Services

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

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

GlobalSign CA issues Certificates in compliance with RFC 5280 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

GlobalSign CA issues Certificates with algorithms indicated by the following OIDs:

- **SHA1WithRSAEncryption** {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
- **SHA256WithRSAEncryption** {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
- **ECDSAWithSHA1** {iso(1) member-body(2) us(840) ansi- X9- 62 (10045) signatures(4) 1 }
- **ECDSAWithSHA224** {iso(1) member- body(2) us(840) ansi- X9- 62 (10045) signatures(4) ecdsa- with- SHA2(3) 1 }
- **ECDSAWithSH256** {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 }

7.1.4 Name Forms

GlobalSign CA issues Certificates with name forms compliant to RFC 5280. Within the domain of each Issuing CA, GlobalSign CA includes a unique non-sequential Certificate serial number that exhibits at least 20 bits of entropy.

7.1.5 Name Constraints

GlobalSign CA may issue Certificates with name constraints where necessary and mark as critical where necessary as part of the Trusted Root program.

7.1.6 Certificate Policy Object Identifier

No stipulation

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

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

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

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:-

- **CRL Number** GlobalSign XXX etc. (Depending upon product)
- **Authority Key Identifier** AKI of the issuing CA for chaining/validation requirements

7.3 OCSP Profile

GlobalSign CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019 and highlights this within the AIA extension via an OCSP responder URL.

7.3.1 Version Number(s)

GlobalSign CA issues Version 1 OCSP responses with following fields:

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

An OCSP request must contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

7.3.2 OCSP Extensions

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

8.0 Compliance Audit and Other Assessments

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

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities (current version: 2.0) AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria (current version: 1.4)
- AICPA/CICA WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria (current version: 1.1)

8.1 Frequency and Circumstances of Assessment

GlobalSign CA maintains its compliance with the AICPA standards identified above via a Qualified Auditor on an annual basis. The audit covers all of GlobalSign CA's activities.

8.2 Identity/Qualifications of Assessor

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

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an internal government auditing agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million ($1,000,000) US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communications of Results

Results of the audit are reported to the Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

GlobalSign CA 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 CA's Certificate status infrastructure.

9.1.4 Fees for Other Services

GlobalSign CA may charge for other additional services such as timestamping.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End Entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by GlobalSign CA staff including Vetting Agents and administrators:

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

GlobalSign CA is responsible for securely storing private information in accordance with a published Privacy Policy document and may store information received in either paper or digital form. Any backup of private information must be encrypted when transferred to suitable backup media. The Privacy Policy is published on GlobalSign CA'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 CA 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 CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

GlobalSign CA 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 CA 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 CA retains ownership of Certificates; however, it grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

GlobalSign CA 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 CA, 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 CA represents and warrants to Certificate Beneficiaries , during the period when the Certificate is valid, GlobalSign CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:-

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

In addition, GlobalSign CA represents and warrants to Certificate Beneficiaries for NAESB Certificates that, during the period when the Certificate is valid, GlobalSign CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:

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

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

- **Legal Existence:** GlobalSign CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- **Identity:** GlobalSign CA has confirmed that, as of the date the Certificate was issued, the legal name of the Subject named in the Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;

- **Right to Use Domain Name:** For EV Certificates only, GlobalSign CA has taken all steps reasonably necessary to verify that, as of the date the Certificate was issued, the Subject named in the Certificate has the right to use all the Domain Name(s) listed in the Certificate;
- **Authorization for EV Certificate:** GlobalSign CA has taken all steps reasonably necessary to verify that the Subject named in the Certificate has authorized the issuance of the Certificate;
- **Accuracy of Information:** GlobalSign CA has taken all steps reasonably necessary to verify that all of the other information in the Certificate is accurate, as of the date the Certificate was issued;
- **Subscriber Agreement:** The Subject named in the Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
- **Status:** GlobalSign CA will follow the requirements of the EV and/or EV Code Signing Guidelines (as applicable) and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the Certificate as Valid or revoked; and
- **Revocation:** GlobalSign CA will follow the requirements of the EV and/or EV Code Signing Guidelines and revoke the Certificate for any of the revocation reasons specified in the EV and/or EV Code Signing Guidelines.

9.6.2 RA Representations and Warranties

RAs warrant that:-

- Issuance processes are in compliance with this CPS and the relevant CP;
- All information provided to GlobalSign CA does not contain any misleading or false information; and
- All translated material provided by the RA is accurate.

9.6.3 Subscriber Representations and Warranties

Subscribers and/or Applicants warrant that:-

- Subscriber will provide accurate and complete information at all times to GlobalSign CA, both in the Certificate Request and as otherwise requested by GlobalSign CA in connection with issuance of a Certificate;
- 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;
- Subscriber shall review and verify the Certificate contents for accuracy;
- Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Subscriber shall promptly cease use of a Certificate and its associated Private Key, and promptly request GlobalSign CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or Compromise of the Subscriber's Private Key associated with the Public Key in the Certificate;
- Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate; and
- Subscriber shall respond to GlobalSign CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours.

Applicant acknowledges and accepts that GlobalSign CA is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if GlobalSign CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.3.1 North American Energy Standards Board (NAESB) Subscribers

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

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

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

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

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

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

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

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

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

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

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

9.6.4 Relying Party Representations and Warranties

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

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

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

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CPS; and

- Take any other precautions prescribed in the Issuing CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

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

9.6.4.1 North American Energy Standards Board (NAESB) Relying Parties

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

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

9.6.4.2 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

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

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

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

9.9 Indemnities

9.9.1 Indemnification by GlobalSign CA

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

9.9.2 Indemnification by Subscribers

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

unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the Compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3 Indemnification by Relying Parties

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

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until such time as communicated otherwise by GlobalSign CA 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 CA will communicate the conditions and effect of this CPS termination via the appropriate Repository.

9.11 Individual Notices and Communications with Participants

GlobalSign CA 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 CA 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 CA must be addressed to: legal@globalsign.com or by post to GlobalSign CA in the address provided in Section 1.5.2.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

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

Upon receipt of a dispute notice, GlobalSign CA convenes a dispute committee that advises GlobalSign CA 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 CA 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 CA executive management. The GlobalSign CA executive management may subsequently communicate the proposed settlement to the complaining party.

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code.

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

For all technology related disputes and disputes related to this CPS the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:

J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel.: +32-47-733 82 96, Fax: + 32-16-32 54 38.

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of GlobalSign CA Certificates or other products and services. The law of Belgium applies also to all GlobalSign CA commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to GlobalSign CA products and services where GlobalSign CA acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including GlobalSign CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Leuven, Belgium.

9.15 Compliance with Applicable Law

GlobalSign CA complies with applicable laws of Belgium. Export of certain types of software used in certain GlobalSign CA public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including GlobalSign CA, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Belgium.

9.16 Miscellaneous Provisions

9.16.1 Compelled Attacks

GlobalSign CA is subject to Belgium jurisdiction and regulatory framework. GlobalSign's CA infrastructure is based in Belgium and France, and RA infrastructure is based in Belgium and Japan. GlobalSign CA's sales offices and/or strategic partners have no access to any part of GlobalSign's CA infrastructure. GlobalSign CA will use all reasonable legal defence against being compelled by a third party to issue Certificates in violation of the CP and CPS.

.

9.16.2 Entire Agreement

GlobalSign CA will contractually obligate every RA involved with Certificate issuance to comply with this CPS and all applicable industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.3 Assignment

Entities operating under this CPS cannot assign their rights or obligations without the prior written consent of GlobalSign CA.

9.16.4 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 effect the original intention of the parties

9.16.5 Enforcement (Attorney's Fees and Waiver of Rights)

GlobalSign CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. GlobalSign CA's failure to enforce a provision of this CPS does not waive GlobalSign CA'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 CA.

9.17 Other Provisions

No Stipulation