GlobalSign CA
Certification Practice Statement

Date: March 15th 2013

Version: v.7.4

Table of Contents

TABLE OF CONTENTS **2**
DOCUMENT HISTORY **6**
DETAILED HISTORY OF CHANGES **7**
ACKNOWLEDGMENTS **8**
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 13
1.3.1 Certification Authorities *13*
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 *19*
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*
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 31
3.3.1 Identification and Authentication for Routine Re-key *31*
3.3.2 Identification and Authentication for Re-key After Revocation *32*
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 32
4.0 CERTIFICATE LIFE-CYCLE 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 34
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 35
4.4.1 Conduct Constituting Certificate Acceptance 35
4.4.2 Publication of the Certificate by the CA 35
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 35
4.5 KEY PAIR AND CERTIFICATE USAGE 35
4.5.1 Subscriber Private Key and Certificate Usage 35
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 36
4.6.3 Processing Certificate Renewal Requests 36
4.6.4 Notification of New Certificate Issuance to Subscriber 36
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 36
4.6.6 Publication of the Renewal Certificate by the CA 36
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 37
4.7.3 Processing Certificate Re-Keying Requests 37
4.7.4 Notification of New Certificate Issuance to Subscriber 37
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 37
4.7.6 Publication of the Re-Keyed Certificate by the CA 37
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 38
4.9.1 Circumstances for Revocation 38
4.9.2 Who Can Request Revocation 39
4.9.3 Procedure for Revocation Request 39
4.9.4 Revocation Request Grace Period 39
4.9.5 Time Within Which CA Must Process the Revocation Request 39
4.9.6 Revocation Checking Requirements for Relying Parties 40
4.9.7 CRL Issuance Frequency 40
4.9.8 Maximum Latency for CRLs 40
4.9.9 On-Line Revocation/Status Checking Availability 40
4.9.10 On-Line Revocation Checking Requirements 40
4.9.11 Other Forms of Revocation Advertisements Available 40
4.9.12 Special Requirements Related to Key Compromise 40
4.9.13 Circumstances for Suspension 40
4.9.14 Who Can Request Suspension 40
4.9.15 Procedure for Suspension Request 40
4.9.16 Limits on Suspension Period 40
4.10 CERTIFICATE STATUS SERVICES 41
4.10.1 Operational Characteristics 41
4.10.2 Service Availability 41
4.10.3 Operational Features 41

4.10.4 End of Subscription *41*
4.11 KEY ESCROW AND RECOVERY 41
4.11.1 Key Escrow and Recovery Policy and Practices *41*
4.11.2 Session Key Encapsulation and Recovery Policy and Practices *41*

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 41

5.1 PHYSICAL CONTROLS 41
5.1.1 Site Location and Construction *41*
5.1.2 Physical Access *41*
5.1.3 Power and Air Conditioning *41*
5.1.4 Water Exposures *42*
5.1.5 Fire Prevention and Protection *42*
5.1.6 Media Storage *42*
5.1.7 Waste Disposal *42*
5.1.8 Off-Site Backup *42*
5.2 PROCEDURAL CONTROLS 42
5.2.1 Trusted Roles *42*
5.2.2 Number of Persons Required per Task *42*
5.2.3 Identification and Authentication for Each Role *42*
5.2.4 Roles Requiring Separation of Duties *42*
5.3 PERSONNEL CONTROLS 43
5.3.1 Qualifications, Experience, and Clearance Requirements *43*
5.3.2 Background Check Procedures *43*
5.3.3 Training Requirements *43*
5.3.4 Retraining Frequency and Requirements *43*
5.3.5 Job Rotation Frequency and Sequence *43*
5.3.6 Sanctions for Unauthorized Actions *43*
5.3.7 Independent Contractor Requirements *43*
5.3.8 Documentation Supplied to Personnel *44*
5.4 AUDIT LOGGING PROCEDURES 44
5.4.1 Types of Events Recorded *44*
5.4.2 Frequency of Processing Log *44*
5.4.3 Retention Period for Audit Log *44*
5.4.4 Protection of Audit Log *44*
5.4.5 Audit Log Backup Procedures *44*
5.4.6 Audit Collection System (Internal vs. External) *44*
5.4.7 Notification to Event-Causing Subject *44*
5.4.8 Vulnerability Assessments *44*
5.5 RECORDS ARCHIVAL 45
5.5.1 Types of Records Archived *45*
5.5.2 Retention Period for Archive *45*
5.5.3 Protection of Archive *45*
5.5.4 Archive Backup Procedures *46*
5.5.5 Requirements for Time-Stamping of Records *46*
5.5.6 Archive Collection System (Internal or External) *46*
5.5.7 Procedures to Obtain and Verify Archive Information *46*
5.6 KEY CHANGEOVER 46
5.7 COMPROMISE AND DISASTER RECOVERY 46
5.7.1 Incident and Compromise Handling Procedures *46*
5.7.2 Computing Resources, Software, and/or Data Are Corrupted *46*
5.7.3 Entity Private Key Compromise Procedures *46*
5.7.4 Business Continuity Capabilities After a Disaster *47*
5.8 CA OR RA TERMINATION 47

6.0 TECHNICAL SECURITY CONTROLS 47

6.1 KEY PAIR GENERATION AND INSTALLATION 47
6.1.1 Key Pair Generation *47*
6.1.2 Private Key Delivery to Subscriber *47*
6.1.3 Public Key Delivery to Certificate GlobalSign CA *47*
6.1.4 CA Public Key Delivery to Relying Parties *47*

6.1.5 Key Sizes 47
6.1.6 Public Key Parameters Generation and Quality Checking 48
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 48
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 48
6.2.1 Cryptographic Module Standards and Controls 48
6.2.2 Private Key (n out of m) Multi-Person Control 48
6.2.3 Private Key Escrow 48
6.2.4 Private Key Backup 48
6.2.5 Private Key Archival 48
6.2.6 Private Key Transfer Into or From a Cryptographic Module 48
6.2.7 Private Key Storage on Cryptographic Module 48
6.2.8 Method of Activating Private Key 48
6.2.9 Method of Deactivating Private Key 49
6.2.10 Method of Destroying Private Key 49
6.2.11 Cryptographic Module Rating 49
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 49
6.3.1 Public Key Archival 49
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 49
6.4 ACTIVATION DATA 49
6.4.1 Activation Data Generation and Installation 49
6.4.2 Activation Data Protection 49
6.4.3 Other Aspects of Activation Data 49
6.5 COMPUTER SECURITY CONTROLS 50
6.5.1 Specific Computer Security Technical Requirements 50
6.5.2 Computer Security Rating 50
6.6 LIFE CYCLE TECHNICAL CONTROLS 50
6.6.1 System Development Controls 50
6.6.2 Security Management Controls 50
6.6.3 Life Cycle Security Controls 50
6.7 NETWORK SECURITY CONTROLS 51
6.8 TIME-STAMPING 51
6.8.1 PDF Signing Time-Stamping Services 51
6.8.2 Code Signing and EV Code Signing Time-Stamping Services 51

7.0 CERTIFICATE, CRL, AND OCSP PROFILES 51

7.1 CERTIFICATE PROFILE 51
7.1.1 Version Number(s) 51
7.1.2 Certificate Extensions 51
7.1.3 Algorithm Object Identifiers 51
7.1.4 Name Forms 51
7.1.5 Name Constraints 52
7.1.6 Certificate Policy Object Identifier 52
7.1.7 Usage of Policy Constraints Extension 52
7.1.8 Policy Qualifiers Syntax and Semantics 52
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 52
7.2 CRL PROFILE 52
7.2.1 Version Number(s) 52
7.2.2 CRL and CRL Entry Extensions 52
7.3 OCSP PROFILE 52
7.3.1 Version Number(s) 52
7.3.2 OCSP Extensions 52

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 52

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT 53
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 53
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 53
8.4 TOPICS COVERED BY ASSESSMENT 53
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 53
8.6 COMMUNICATIONS OF RESULTS 53

9.0 OTHER BUSINESS AND LEGAL MATTERS 53

9.1 FEES 53
9.1.1 Certificate Issuance or Renewal Fees 53
9.1.2 Certificate Access Fees 53
9.1.3 Revocation or Status Information Access Fees 53
9.1.4 Fees for Other Services 53
9.1.5 Refund Policy 53
9.2 FINANCIAL RESPONSIBILITY 54
9.2.1 Insurance Coverage 54
9.2.2 Other Assets 54
9.2.3 Insurance or Warranty Coverage for End-Entities 54
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 54
9.3.1 Scope of Confidential Information 54
9.3.2 Information Not Within the Scope of Confidential Information 54
9.3.3 Responsibility to Protect Confidential Information 54
9.4 PRIVACY OF PERSONAL INFORMATION 54
9.4.1 Privacy Plan 54
9.4.2 Information Treated as Private 54
9.4.3 Information Not Deemed Private 54
9.4.4 Responsibility to Protect Private Information 54
9.4.5 Notice and Consent to Use Private Information 55
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 55
9.4.7 Other Information Disclosure Circumstances 55
9.5 INTELLECTUAL PROPERTY RIGHTS 55
9.6 REPRESENTATIONS AND WARRANTIES 55
9.6.1 CA Representations and Warranties 55
9.6.2 RA Representations and Warranties 56
9.6.3 Subscriber Representations and Warranties 56
9.6.4 Representations and Warranties of Other Participants 58
9.7 DISCLAIMERS OF WARRANTIES 58
9.8 LIMITATIONS OF LIABILITY 58
9.9 INDEMNITIES 58
9.9.1 Indemnification by GlobalSign CA 58
9.9.2 Indemnification by Subscribers 58
9.9.3 Indemnification by Relying Parties 59
9.10 TERM AND TERMINATION 59
9.10.1 Term 59
9.10.2 Termination 59
9.10.3 Effect of Termination and Survival 59
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 59
9.12 AMENDMENTS 59
9.12.1 Procedure for Amendment 59
9.12.2 Notification Mechanism and Period 59
9.12.3 Circumstances Under Which OID Must be Changed 59
9.13 DISPUTE RESOLUTION PROVISIONS 59
9.14 GOVERNING LAW 60
9.15 COMPLIANCE WITH APPLICABLE LAW 60
9.16 MISCELLANEOUS PROVISIONS 60
9.16.1 Compelled Attacks 60
9.16.2 Survival 60
9.16.3 Entire Agreement 60
9.16.4 Assignment 60
9.16.5 Severability 60
9.16.6 Enforcement (Attorney's Fees and Waiver of Rights) 60
9.17 OTHER PROVISIONS 60

Document History

Version	Release Date	Author	Status + Description

V.5.0	10/07/05	Andreas Mitrakas	Draft
	30/08/05	Jean-Paul Declerck	Final version
	02/02/06	Johan Sys	Administrative clean-up
v.5.1	13/03/06	Johan Sys	Added GlobalSign Educational ServerSign
v.5.2	29/11/06	Philippe Deltombe	Added GlobalSign OrganizationSSL
	6/12/06	Johan Sys	Removed SureServer products
v.5.3	23/01/07	Johan Sys	Added GlobalSign DomainSSL Added GlobalSign Root CA R2 Adjusted liability gaps
v.5.4	30/3/07	Johan Sys	Administrative update / clarifications
v.5.5	19/6/07	Johan Sys	Renamed product names
v.5.6	25/06/07	Steve Roylance	Final modification for EV Issue 1.0
v.6.0	17/12/07	Steve Roylance	Major Release supporting new certificate lifecycle solutions
v.6.1	20/05/08	Steve Roylance	Administrative update/ clarifications
v.6.2	13/10/08	Steve Roylance	Administrative update/ clarifications
v.6.3	16/12/08	Steve Roylance	Administrative update/ clarifications
v.6.4	11/02/09	Steve Roylance	Administrative update/clarifications
v.6.5	12/05/09	Steve Roylance	Administrative update/clarifications
v 6.6	03/02/10	Lila Kee	Administrative update
v 6.7	12/05/10	Johan Sys	Administrative update/clarifications
v 7.0	22/03/12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CABForum Minimum Guidelines for issuance of SSL certificates
v 7.1	29/03/12	Lila Kee and Steve Roylance	Addition of support for NAESB and Incorporation of the AlphaSSL product range
v 7.2	07/06/12	Steve Roylance	Additional CABForum requirements
V 7.3	01/07/12	Steve Roylance	Final CABForum requirements
V7.4	03/15/13	Giichi Ishii Lila Kee	Extended validity period of Personal Sign, Administrative updtates/clarifications Modification to NAESB certificates incorporating WEQ-012 v 3.0 updates

Detailed History of Changes

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 CABForum Minimum Guidelines provisions – C name checking

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

- Endorsement of additional CABForum Minimum Guidelines provisions

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 TrustedRoot 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 Limited 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 endorses in whole or in part the following industry standards:

- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).
- The ISO 1-7799 standard on security and infrastructure
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- X509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) Standards – WEQ-012

This CPS is assessed according to the requirements of the following schemes and endorses these in whole or in part:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities.
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria.
- CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

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 Digital Certificates including validity checking services. GlobalSign nv/sa may also provide additional services such as time-stamping. 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, however, this version remains the primary source).*

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 policy according to the structure of RFC 3647, the topic may not necessarily apply to Services of GlobalSign nv/sa. These sections have *'No stipulation'* appended. 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 on the practices and procedures. 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 the GlobalSign CA during the complete life cycle of certificates issued by the GlobalSign CA.

The 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 Agreement. For Relying Parties this CPS becomes binding by relying upon a certificate issued under this CPS. In addition, Subscribers are bound 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 digital 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 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 applies to the above-stated domain to the exclusion of any other. This CPS aims at facilitating the GlobalSign CA in delivering certification services and managing the certificate lifecycle of any issued 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	A personal certificate of medium assurance with reference to professional context
PersonalSign 2 Pro DepartmentSign	A 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 bespoke Certificate Authority created as a trust anchor issuing PersonalSign 2 Pro
DomainSSL	A certificate to authenticate web servers
AlphaSSL	A certificate to authenticate web servers

OrganizationSSL	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 *
Digital IDs for 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 Certificate Authority as designated by the North American Energy Standards Board
PDF Signing for Adobe CDS**	
PersonalSign for Adobe CDS	A certificate of medium hardware assurance chained to the Adobe Root CA which may have reference to a professional context.
PersonalSign Pro 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.
DepartmentSign for Adobe CDS	A personal digital ID issued with reference to professional context for the purpose of signing Adobe PDF documents
TrustedRoot for Adobe CDS	A role-based certificate with reference to professional context for the purpose of signing Adobe PDF documents
TimeStamping for Adobe CDS	A level 2 intermediate CA that enters the GlobalSign CA for Adobe hierarchy
Test Digital ID for Adobe CDS	A certificate to authenticate time sources A certificate for test or demonstration purposes which does not require hardware Assurance. .

* These certificates are issued and managed in accordance with CA/Browser Forum Guidelines for Extended Validation Certificates, which are incorporated by reference into this CPS.
The remaining certificate types shall be issued and managed in accordance with CA/Browser Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates if so indicated by the inclusion of CA/Browser Forum Policy OIDs as detailed in section 1.2.
** These certificates are issued and managed in accordance with the Adobe Systems Incorporated Certificate Policy 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 for them
- 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.
- Can be used for encryption of data.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, 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 the GlobalSign CA uses in creating and maintaining the certificates that it manages. In addition to the CP and CPS GlobalSign CA maintains a range of adjacent documented polices which include but are not limited to addressing such issues as:

- Business Continuity and Disaster Recovery
- Security Policy
- Personnel Policies
- Key management Policies
- Registration Procedures

Additionally, other pertinent documents include:

- The GlobalSign Limited Warranty Policy that addresses issues on insurance.
- The GlobalSign Privacy Policy on the protection of personal data
- The GlobalSign Certificate Policy that addresses the trust objectives for the domain of the GlobalSign top roots.

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 notices with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the hierarchy. This includes the Root CA as well as any operational certificates. This can be established on the basis of the assertions within this CPS.

All applicable GlobalSign CA policies have been subjected to continuous audit and scrutiny of authorised third parties, which GlobalSign CA highlights on its public facing web site via a WebTrust site seal. Additional information can be made available upon request.

1.1.1 Certificate Naming

The exact names of the GlobalSign CA certificates that make use of 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
- North American Energy Standards Board Inc. Issuing CA – SHA256 – G2
- AlphaSSL G2 with serial number 04 00 00 00 00 01 2F 4E E1 37 02

GlobalSign CA actively promotes the inclusion of the 5 Root certificates above (R1-R5) into hardware and software platforms that are capable of supporting digital 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 lifecycle management. However, GlobalSign CA also actively encourages platform providers at their own discretion to include GlobalSign CA Root certificates without contractual obligation.

TrustedRoot is a GlobalSign CA service, which allows third-party Issuer CAs to chain to one of the GlobalSign CA Root certificates. 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 [2]

TrustedRoot 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.

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data digitally. By means of a digital certificate, GlobalSign CA provides confirmation of the relationship between a named entity (subscriber) and its public key. The process to obtain a digital certificate includes the identification, naming, authentication and registration of the client as well as aspects of certificate management such as the issuance, revocation and expiration of the digital certificate. By means of this procedure to issue digital certificates, GlobalSign CA provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such an entity uses. GlobalSign CA makes available digital 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

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

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 actively forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection and therefore seeks to maintain a position of leadership with regard to inclusion of its Roots in third party applications.

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 a 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 (Which may be updated from time to time) 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
1.3.6.1.4.1.4146.1.10.20	~~Domain Validation Certificates Policy – SignTrust~~ *(DEPRECATED)*
1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy
1.3.6.1.4.1.4146.1.30	Time Stamping Certificates Policy
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 – TrustedRoot™
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	TrustedRoot 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 North American Standard's Board Certification Authority Accreditation Specification will include the following identifiers as follows:-

2.16.840.1.114505.1.12.1.2	NASESB 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 CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates will include the additional identifiers as follows:-

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 additional identifiers as follows:-

1.2.840.113583.1.1.5	Adobe Certified Document Services OID

1.3 PKI participants

1.3.1 Certification Authorities

GlobalSign CA is a Certification Authority that issues high quality and highly trusted certificates in accordance with this CPS. As a Certificate Authority, GlobalSign CA performs functions related to PKI certificate LiveCycle Management such as subscriber registration, certificate issuance, certificate renewal, certificate distribution and certificate revocation. GlobalSign CA also provides Certificate status information using an online repository in the form of a CRL (Certificate Revocation List) distribution point and/or OCSP (Online Certificate Status Protocol) 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 an RA (Registration Authority) 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 Certification Practice Statement relating to all digital certificates in the GlobalSign CA hierarchy. Through its Policy Authority

GlobalSign CA has ultimate control over the lifecycle and management of the GlobalSign Root and any subsequent subordinate issuing CA including TrustedRoot 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 to GlobalSign CA on the basis of a service agreement. The scope is certificate issuance and revocation services. The GlobalSign CA outsources 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 services and certificates on behalf of GlobalSign CA. GlobalSign CA outsource agents are located in Belgium and France.

GlobalSign CA is also a Time Stamping 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 Root, 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

A Registration Authority (RA) is an entity that identifies and authenticates applicants for certificates. A RA may also initiate or pass along revocation requests for certificates and requests for re-issuance and renewal (sometimes referred to as rekey) of certificates. GlobalSign CAs may act as a Registration Authority for certificates it issues in which case they are 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 a subscriber's application.
- Following approval of an application requesting issuance of a certificate via a multifactor authentication process.
- Initiating the process to revoke a certificate from the applicable GlobalSign CA subordinate issuing 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 abide by all the requirements of the CPS and the terms of their contract which may also refer to additional criteria as recommended by the CABForum. RA's may implement more restrictive vetting practices if their internal policy dictates.

In order to issue certain specific certificate type, RAs might need to rely on certificates issued by third party certification authorities or other third party databases and sources of information. Identity cards and drivers licenses are such sources of authoritative subscriber information. Relying Parties are hereby prompted to seek specific information by referring to this Certification Practice Statement.

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 GCC (GlobalSign Certificate Centre) configuration. These entities are also usually known as Enterprise RAs.

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

For the issuance of ExtendedSSL certificates and Extended Validation Code Signing, GlobalSign CA contractually obligates each RA and/or subcontractor to comply with all applicable requirements in the EV Guidelines incorporated by reference herein, and to perform them as required.

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 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 technically enforces this.

GlobalSign CA shall not delegate the performance of the Final Cross-Correlation and Due Diligence requirements of Section 24 of Extended Validation Guidelines.

1.3.3 Subscribers

Subscribers to GlobalSign CA are either legal persons or natural persons that successfully apply for and receive a certificate to support their use in transactions, communications and the application of digital signatures.
The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the GlobalSign CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

Legal persons are identified on the basis of the published by-laws and appointment of Director as well as the subsequent government gazette or other QIIS or 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 on the online process for the application for a certificate.

Subscribers of end entity certificates issued under the 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 an employment or service agreement or otherwise a pre-existing contract relationship with GlobalSign CA authorising it to carry out a specific function within the scope of an application that uses GlobalSign CA certificate services. Granting 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

Relying parties are natural persons or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate, relying parties must always refer to GlobalSign CA's revocation information either in the form of a Certificate Revocation List (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 document. It is best practice for certifying authors to include certificate status information and an appropriate time stamp within a signed PDF. Such additional detail may be inspected by relaying parties through 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-----
MIIFJjCCAw6gAwIBAgIKYSkVJwAAAAAKjANBgkqhkiG9w0BAQUFADB/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 digital certificate is a specifically formatted data object that cryptographically binds an identified subscriber with a Public Key (supporting either RSA or ECC). A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital 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, electronic mail etc. The signature certificate is only warranted to produce digital signatures in the context of applications that support digital certificates. Certificates 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)
- **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 digital ID be used for encryption due to the singularity of the digital ID 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 digital certificate can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a digital certificate. To describe the function of authentication, the term digital signature is often used.

- **PersonalSign 1:** authentication of the existence of an email address
- **PersonalSign 2:** authentication of a natural person (medium level assurance)
- **PersonalSign 2 Pro:** authentication of a natural person within an organizational context or a role within an organizational context(medium level assurance)
- **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)

- **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 identifying of web sites and other on line resources, such as software objects etc. The authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used.

- **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.
- **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 NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB Medium** authentication as prescribed NIST SP800-63 version 1.0.2 section 7.2.1
- **NAESB High** authentication as prescribed NIST SP800-63 version 1.0.2 section 7.2.1

Assurance levels: Subscribers should choose an appropriate level of assurance to which relying parties will confidently transact. For example Subscribers with an unknown brand name should positively assure relying parties of their identity with a High Assurance (EV) certificate where as a closed community with a well-known URL may chose a Low Assurance solution.

- **Low assurance:** (Class 1) certificates are not suitable for identity verification as no authenticated identity information is included within the certificate. This in turn does not support non repudiation services.
- **Medium assurance:** (Class 2) certificates are individual and organizational certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances 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 in comparison with Class 1 and 2.
- **High assurance (EV):** (Extended Validation) certificates are Class 3 certificates issued by GlobalSign CA in conformance with the Guidelines for Extended Validation Certificates.
- **NAESB Rudimentary** This level provides the lowest degree of assurance concerning the identity of the end entity. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to 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 relevant to 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 relevant to 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 time-stamping and code signing certificates, can be used to ensure the confidentiality of communications effected by means of digital 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 Business Practice Standards WEQ-012 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
- Any transaction or data transfer deemed illegal under federal law.

Any other use of a digital certificate is not supported by this CPS. When using a digital 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 Limited 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,
  - any other system whose failure could lead to injury, death or environmental damage;
- 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. EKU = Enhanced or Extended Key usage

- PersonalSign 1 and Demo - Client Authentication and Secure email EKU
- PersonalSign 2 / 2 Pro - 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* - Client and Server Authentication EKU
- DomainSSL* - Client and Server Authentication EKU
- AlphaSSL* - Client and Server Authentication EKU
- ExtendedSSL* - Client and Server Authentication EKU
- Time-stamping - Time-stamping EKU
- Code Signing and EV Code Signing - Code Signing EKU
- PDF Signing - Adobe CDS Document Signing EKU
- TrustedRoot - All policies

** SGC (Server Gated Cryptography may also be set for backwards compatibility)*

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 key.
- To show the number of levels in the hierarchy under a CA certificate.
- To constrain a TrustedRoot CA Certificate to a customer's specific Domain

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Principle 1 Policy Authority
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

The Principle 1 Policy Authority determines the suitability and applicability of the CP and the conformance of this CPS based on the results and recommendations received from an independent WebTrust auditor. Each Policy Authority, as described below, is responsible for evaluating and acting upon the results of compliance audits.

In an effort to invoke credibility and Trust in this CPS and to better correspond to accreditation and legal requirements, the Policy Authority may make revisions and updates to policies as it sees fit or as required by other circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of this CPS.

New versions and publicized updates of appropriate policies are approved by one of three Policy Authorities which relate to either, Public Practices *(WebTrust Principle 1 Policy Authority),* Vetting Practices *(WebTrust Principle 2 Policy Authority)* or Security Practices *(WebTrust Principle 3 Policy Authority).* Each Policy Authority in its present organisational structure comprises members as indicated below:

- At least one member of the management of GlobalSign CA or a GlobalSign group company.
- At least two authorised agents directly involved in the drafting and development of GlobalSign CA practices and policies.

The Management member chairs the applicable Policy Authority ex officio and each Policy Authority reports to the Board of Directors of GlobalSign nv/sa.

All members of each Policy Authority have one vote to determine the suitability of the Policy. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chair of the Policy Authority counts double.

Each Policy Authority chair is also responsible for implementation of any independent third party auditor feedback into applicable polices.

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 online Repository at https://www.globalsign.com/repository.

The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the CPS.

Subscribers that are affected by changes may file comments with the policy administration organization within 15 days from notice. Only subscribers and the supervisory authority (Webtrust Auditor) may submit objections to policy changes. Relying parties that are not subscribers do not have the right to submit objections.

GlobalSign CA publishes on its web site the two latest versions of this CPS.

1.5.4.1 Changes with notification

Updated versions of this CPS are notified to parties that have a legal duty to receive such updates, for example auditors with a specific mandate to do so.

1.5.4.2 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.6 Definitions and acronyms

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

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.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate Request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

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 Information is correct.

Audit Criteria: The requirements described in this document and any requirements that an entity must follow in order to satisfy the audit scheme selected under section 16.1

Audit Report: A statement, report, or letter issued by a Qualified Auditor stating a CA's or RA's compliance with these Requirements.

Binding: A statement by an RA of the relationship between a named entity and its public key.

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

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

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

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

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

Certificate Revocation List: A regularly updated time-stamped 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.

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 Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a certificate for a specific Domain Namespace.

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

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).

Effective Date: The date, as determined by the eligible audit schemes, on which Requirements come into force.

Enterprise Certificate: A Certificate whose issuance is authorized by an Enterprise RA.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

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.

HSM: Hardware Security Module: A 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.

Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

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.

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.

Independent Audit: An audit that is performed by a Qualified Auditor and that determines an entity's compliance with these Requirements and one or more of the audit schemes listed in Section 16.1.

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): Public Key Infrastructure (PKI) Standards – WEQ-012 v3.0: 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

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

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

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

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

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

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

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

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.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

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.

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

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 or Terms of Use Agreement.

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

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

TPM: Trusted Platform Module – 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.

Validation Specialists: Someone who performs the information verification duties specified by these 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 digital certificates.

AICPA	American Institute of Certified Public Accountants
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
ETSI	European Telecommunications Standards Institute
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GSCA	GlobalSign Certification Authority
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IM	Instant Messaging
ISO	International Organization for Standardization

ISO	International Standards organization
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
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
VOIP	Voice Over Internet Protocol

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 online repositories. GlobalSign CA ensures that revocation data for issued certificates and its roots 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 down - time 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 certain elements of documentation including security controls, procedures, internal security polices etc. However elements may be disclosed in audits associated with formal accreditation schemes that GlobalSign CA adheres to, such as WebTrust for CAs and WebTrust for EV.

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 the in the event of a dispute, the English version shall be deemed the master.

2.2 Publication of Certificate Information

GlobalSign CA publishes its CP, CPS, Subscriber Agreements, and Relying Party Agreements on https://www.globalsign.com/repository. CRLs are published in online repositories. The CRLs contain entries for all revoked un-expired certificates and are valid, depending on certificate type.

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 Warranties are published within seven days after being digitally signed by the CPS (Principle 1 Policy Authority) using an Adobe CDS PDF signing certificate with appropriate time stamp.

2.4 Access control on repositories

While GlobalSign CA strives to keep access to its public repository and access to its policy is (e.g. CP, CPS etc.) free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc.
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 operates an RA that verifies and authenticates the identity and/or other attributes of an Applicant applying for a certificate.

Certificate Applicants are prohibited from using names in their certificate that infringe upon the Intellectual Property Rights of others. GlobalSign CA does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in the certificate application or arbitrates, mediate or otherwise resolve any dispute concerning the ownership of any domain name, trademark, trade name or service mark. GlobalSign CA is entitled without liability to any Certificate 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 publically 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 space 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 Issuer of a certificate. In cases where a GlobalSign CA product allows the use of role or departmental name then additional unique elements may be added to the DN within the OU field to allow differentiation 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 or following a reasoned and legitimate request

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 e-mail address only.
- **PersonalSign/Pro Certificates -** A unique e-mail address coupled with an organizations name and address plus either the name of and individual or a department associated with the organization. Alternatively a unique e-mail address and an individual’s name and country.

- **Code Signing Certificates -** A unique organization name and address or a unique individual name and address with an optional e-mail address.
- **SSL Certificates -** A domain name within the Common Name attribute as approved as unique by ICANN, the Internet Corporation for Assigned names and Numbers.
- **Time Stamping Certificates -** A unique organization name and address with an optional e-mail address.
- **CA for AATL Certificates -** A unique e-mail address coupled with an organizations name and address plus either the name of an individual or a department associated with the organization. Alternatively a unique e-mail address and an individual's name and country.
- **NAESB Rudimentary -** A unique e-mail address only.
- **NAESB Basic, Medium, and High** A unique e-mail address coupled with an organizations name and address plus either the name of an individual or a department associated with the organization.
-
-
- **PDF Signing Certificates -** A unique e-mail address coupled with an organizations name and address plus either the name of an individual or a department associated with the organization. Alternatively a unique e-mail address and an individual's name and country.
- **TrustedRoot -** Following CABForum Base 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. Unless otherwise specifically stated GlobalSign CA does not require that an Applicant's right to use a trademark be verified. GlobalSign CA has 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 for a certificate or for services including CA chaining services using any legal means of communication or investigation necessary to identify the legal person 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 GCC (GlobalSign Certificate Centre) Account is used to authenticate the use of any previously verified information for returning Applicants noting that the aging requirements of section 3.3.1 are upheld by the Account.

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 CSR (Certificate Signing Request) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

GlobalSign CA accepts other Issuer CAs wishing to enter its hierarchy though the TrustedRoot program. Following an initial assessment and signing of a specific agreement with GlobalSign CA the Issuer 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 organisation (which has been authenticated) and GlobalSign CA has been executed.

3.2.2 Authentication of Organization Identity

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 other than Extended Validation, the Legal existence, Legal name, Legal form and requested address of the Organization is verified using one of the following:-

- A Government agency in the jurisdiction of the applicant;
- A third party data base 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 Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information

Alternatively, 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.

For SSL/TLS Certificates, the applicant's ownership or control of all requested Domain(s) is authenticated by one of the following methods;

- Using GlobalSign's OneClickSSL protocol whereby the applicant is required to demonstrate control of a domain by installing a non publically trusted test certificate of GlobalSign CA's design, or;
- By uploading specific meta-data to a defined page on the domain, or;
- By direct confirmation with the contact listed by the Domain Name Registrar in the WHOIS record, or;
- By successfully replying to a challenge response e-mail 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 e-mail 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 aging requirements of 3.3.1
- By receiving a reliable communication from the Domain Name Registrar stating that the Registrant gives the Applicant permission to use the Domain

Further information may be requested from the applicant and other information and or methods may be utilized in order to demonstrate an equivalent level of confidence.

3.2.2.1 Local Registration Authority Authentication

For ePKI and MSSL accounts, GlobalSign CA fixes 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 to 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 Role Based Certificates are authenticated. LRAs are contractually obligated to ensure that Role Based names relating to the Organization Profile and its business are accurate and correct.

Role based Certificates are not be made available to individuals.

3.2.2.3 Extended Validation Certificates (SSL and Code Signing)

For Extended Validation Certificates, the CAB Forum EV guidelines are followed.

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 & 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 (Drivers 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 number from a reliable source, or;
- Performing a postal challenge to the Applicant using an address obtained from a reliable source, or;
- Receiving an attestation from an appropriate Notary, 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 (Drivers 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 be bound to the Organizational subject by one of the following methods;

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

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 fixes authenticated Organizational details in the form of a Profile. Suitably authenticated Account Administrators acting in the capacity of a Local Registration Authority are contractually obliged to authenticate individuals affiliated to the Organization.

3.2.3.5 North American Energy Standards Board (NAESB) Certificates

For NAESB certificate requests, Authenticity of Organization Identity Requests for Subscriber Certificates in the name of an affiliated organization shall include the organization name, address, and documentation of the existence of the organization. GlobalSign or 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 through its ePKI service. 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 Authorized CA Accreditation Specification. 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 Authorized CA 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. Process information shall depend upon the Certificate level of assurance and shall be addressed in the NAESB Authorized CA

accreditation requirements. The documentation and authentication requirements shall vary depending upon the level of assurance.

Registration of Identity Proofing Requirements shall use the using 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 following 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 [1] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.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 highlight Non Verified Subscriber Information to relying parties or to highlight 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 the 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 also omits any disclaimer but notes within this CPS that this item is therefore classified as Non Verified Subscriber Information. 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. CABForum Base Requirement guidelines define the timelines for which these types of objects may be included within certificates and again these items may be classified as Non Verified Subscriber Information.

Specifically for SSL/TLS certificates and Code Signing Certificates, GlobalSign CA maintains an enrolment 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 obliged 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 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 e-mail 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 the e-mail address to be listed within the certificate.
- **NAESB Certificates** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has control over the e-mail address if to be listed within the certificate as detailed in 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 e-mail 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 e-mail 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.
- **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 publically trusted test certificate of GlobalSign CA's design,
  - By uploading specific meta-data 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 e-mail 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 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 e-mail address to be listed within the certificate.
- **PDF Signing Certificates -** Verification through a reliable means of communication with the organization or individual applicant.
- **TrustedRoot -** Verification through a reliable means of communication with the organization's applicant.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Re-key Requests

GlobalSign CA supports re-key requests from subscribers prior to the expiry of the subscribers existing certificate. GlobalSign CA also supports re-issue requests at any time during the lifetime of the certificate. Re-issue is a form of rekey, 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 GlobalSign's Certificate Centre (GCC) re-key is called re-new.

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.
- **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.
- **DV SSL Certificates -** Username and Password required with re-verification every 5 years.
- **OV SSL 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.
- **Time Stamping Certificates -** Not supported
- **CA for AATL Certificates -** Username and Password required with re-verification every 6 years.
- **PDF Signing Certificates -** Not supported.
- **TrustedRoot -** 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 signature key.
Basic	Identity may be established through use of current signature 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 signature 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 signature key, except that identity shall be established through initial registration process at least annually.

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.

Re-verification and Revalidation of Identity When Certificate Information Changes

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

3.3.2 Identification and Authentication for Re-key After Revocation

GlobalSign CA supports rekey for certificates that have not been revoked. Revocation of a certificate mandates the subscriber to follow the initial validation process that was 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 a suitable username and password,

proving possession of unique elements incorporated into the certificate e.g. domain name or e-mail 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.
- **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 Certificates -** Username and Password or out of band.
- **EV SSL Certificates -** Username and Password or out of band.
- **Time Stamping Certificates -** Out of band process.
- **CA for AATL Certificates -** Username and Password or out of band.
- **PDF Signing Certificates -** Username and Password or out of band.
- **TrustedRoot -** Out of band process.

GlobalSign CA may also perform revocation on behalf of subscribers in line with requirements highlighted within its subscriber agreements. Examples include a breach of the subscriber agreement or non-payment of applicable fees.

4.0 Certificate Life-Cycle 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 recognised 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.
Extended Validation rules highlight the specific rules to follow in order to obtain an Extended Validation SSL or Code Signing certificate. Applicants must submit and agree to appropriate 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 from one of four scenarios:-

- **On-line:** Via a web interface over a https session. A certificate 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 and it is known as GCC (GlobalSign Certificate Centre). It requires users to maintain an account with suitably strong username and password for on-going 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 TrustedRoot Program, to 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 e-mail 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 all communications and securely store all information presented by the applicant during the application process.

Generally the application process includes the following steps but not necessarily in this order as some workflow processes generate keys 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 information
- Agreeing to a Subscriber Agreement or applicable Terms and Conditions
- Paying any Applicable Fees

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

GlobalSign CA maintains systems and processes that sufficiently authenticate the applicants identity in line with the applicable statements made in this CPS. Initial identity vetting may be performed by GlobalSign CA's Validation team in line with 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 GlobalSign Certificate Centre (GCC) web interface or through a partner using the GlobalSign CA Application Programming Interface (API). Future applications for certificates are authenticated using single (username and password) or multi factor (Digital 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 requests for certificates from applicants who have previously been rejected or have previously violated a stipulation within their Subscriber Agreement.

Please note that for Extended Validation certificates (SSL and Code Signing) separation of duties is required requiring 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 on why a request has been rejected.

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 occur which are outside of the control of GlobalSign CA, then 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.

- **NAESB Certificates -** Approximately 24-48 business hours
- **PersonalSign3 Pro Certificates -** Approximately 48-72 business hours.
- **Code Signing Certificates -** Approximately 24-48 business hours.
- **EV Code Signing Certificates -** Approximately 48-96 business hours.
- **DV SSL Certificates -** Approximately* 1-5 minutes.
- **AlphaSSL Certificates -** Approximately* 1-5 minutes.
- **OV SSL Certificates -** Approximately 24-48 business hours.
- **EV SSL Certificates -** Approximately 48-96 business hours.
- **Time Stamping Certificates -** Approximately 5-10 business days.
- **CA for AATL Certificates -** Approximately 24-48 business hours.
- **PDF Signing Certificates -** Approximately 24-48 business hours.
- **TrustedRoot -** 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 multifactor authentication. This includes RAs directly operated by GlobalSign CA or RAs contracted by GlobalSign CA. Enterprise or Local RA capabilities do not directly communicate to the CA and therefore multifactor 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 unauthorised modification or tampering.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

GlobalSign CA shall inform the subscriber of the issuance of a certificate to an e-mail address which was supplied by the subscriber during the enrollment process or by any other equivalent method. The e-mail 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 they may not use the Digital Certificate until they have reviewed and verified the accuracy of the data incorporated into the Digital Certificate. Without reaction from the Subscriber within 7 days from receipt, the Digital 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 enrolment.

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 digital 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 Key, Subscribers must securely delete the 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 digital 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 digital certificate from the 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
- **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 Certificates** - Renewal Supported as a Re-Key via GCC
- **EV SSL Certificates -** Renewal Supported as a Re-Key via GCC
- **Time Stamping 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 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
- **TrustedRoot -** 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.
- 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 rekeyed (subject to the points above). The original certificate may be revoked after renewal is complete; however, the original certificate must not be further renewed, rekeyed 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 Re-issue.

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

- **PersonalSign1 Certificates** - Re-Key and Re-Issue Supported via GCC
- **PersonalSign2 Certificates -** Re-Key and Re-Issue Supported via GCC
- **PersonalSign2 Pro Certificates -** Re-Key and Re-Issue Supported via GCC
- **PersonalSign3 Pro Certificates -** Re-Key and Re-Issue Supported via GCC
- **Code Signing Certificates -** Re-Key and Re-Issue Supported via GCC
- **EV Code Signing Certificates -** Re-Key and Re-Issue Supported via GCC
- **DV SSL Certificates -** Re-Key and Re-Issue Supported via GCC
- **AlphaSSL Certificates -** Re-Key and Re-Issue Supported via GCC.
- **OV SSL Certificates** - Re-Key and Re-Issue Supported via GCC
- **EV SSL Certificates -** Re-Key and Re-Issue Supported via GCC
- **Time Stamping Certificates -** Re-Key and Re-Issue Supported via Manual Processes
- **NAESB Certificates** Re-Key and Re-Issue Supported via GCC
- **CA for AATL Certificates -** Re-Key and Re-Issue Supported via GCC
- **PDF Signing Certificates -** Re-Key and Re-Issue Supported via GCC
- **Managed SSL (MSSL) -** Functions are built in to the product
- **Enterprise PKI (ePKI) -** Functions are built in to the product
- **TrustedRoot -** Re-Key and Re-Issue 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.
- 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 rekeyed (subject to the points above). The original certificate may be revoked after rekey is complete; however, the original certificate must not be further renewed, rekeyed 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 key material 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 re-issue request and may re-validate the Subscriber subject to aging restrictions of any previously validated data. In the case of a re-issuance, 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 the 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 rekeyed. The original certificate may be revoked after modification is complete, however, the original certificate cannot be further renewed, rekeyed 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 (Certificate Revocation List). The CRL itself will then be digitally signed with the same key material which originally signed the certificate to be revoked. Adding a serial number allows relying parties to establish that the lifecycle of a digital 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 may be performed under the following circumstances:-

- The Subscriber or Organization Administrator requests revocation of the Digital Certificate through a GlobalSign Certificate Centre (GCC) account which controls the lifecycle of the Digital Certificate,
- The Subscriber requests revocation of the Digital 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 obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised, created using a weak algorithm, or that the Digital Certificate has otherwise been misused,
- GlobalSign CA receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement,
- GlobalSign CA receives notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, certifying or signing malware etc.,
- GlobalSign CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use any of the elements within the 'Subject' or 'Subject Alternative Name' of the Digital Certificate, or that the Subscriber has failed to renew or maintain control of any of those elements,
- GlobalSign CA receives notice or otherwise becomes aware of a material change in the information contained in the Digital Certificate,

- A determination, in GlobalSign CA's sole discretion, that the Digital Certificate was not issued according to best practice or any of GlobalSign CA's own published policies,
- If GlobalSign CA determines that any of the information appearing in the Digital Certificate is not accurate,
- GlobalSign CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Digital Certificate,
- GlobalSign CA's right to issue Digital Certificate expires or is revoked or terminated,
- GlobalSign CA's Private Key for the relevant issuing CA Certificate is compromised,
- GlobalSign CA receives notice or otherwise become aware that a 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,
- The continued use of the certificate is harmful to the business of GlobalSign CA and relying parties.
- The subscriber suspects the loss of a pass phrase to any hardware token which therefore leads to the loss of control of the private key on the token.

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.

For any TrustedRoot CA, GlobalSign CA may revoke the Issuing CA:

- If the TrustedRoot CA no longer meets the contractual terms and conditions of the agreement between the two parties,

4.9.2 Who Can Request Revocation

GlobalSign CAs 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 CAs 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 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 e-mail address.
GlobalSign CAs 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 24-48 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 (twenty-four) 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 30 minutes of receipt.

GlobalSign CA through it's Trusted Root Program processes revocation requests within 24 hours of a confirmation of compromise and a 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 as well as ensuring 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 perform 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 located at: - http://crl.adobe.com/cds.crl

4.9.7 CRL Issuance Frequency

GlobalSign CA meets the requirements of the CABForum Base Requirements for Publically Trusted Certificates and/or the CABForum Requirements for Extended SSL certificates with respect to CRL issuance frequency. GlobalSign's Roots 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 CAs previous CAs which no longer issue are valid between 1 week and 1 month.

4.9.8 Maximum Latency for CRLs

GlobalSign CA ensures that online CA CRLs are published every 3 hours. A request for revocation received from GlobalSign's RA system during the 3 hour period prior to the next scheduled CRL is included within the CRL if received up to 30 minutes prior.
Where GlobalSign CA cross signs other CAs through the TrustedRoot program, it will revoke within 24 hours of a confirmation of compromise and publish an ARL within 12 hours of its creation.

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.

4.9.10 On-Line Revocation Checking Requirements

Relying parties must confirm revocation information otherwise all warranty 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 Digital 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 TrustedRoot, contracts between parties must be maintained throughout the life of the certificate, unless revocation is used 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, etc. 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 life cycle 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 media is protected against obsolescence and deterioration of the media within a defined period of time and 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 life cycle 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 digital certificates via a suitable RA system

5.2.2 Number of Persons Required per Task

GlobalSign CA requires at least 2 people per task. The goal is to guarantee the trust for all CA services (key 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 designated to the roles defined in section 5.2.1 above. It is forbidden to own at the same time the following roles:

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

No individual shall be assigned more than one identity.

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 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 roles or management any person who is known to have a conviction for a serious crime or another offence, which affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed. GlobalSign CA requires candidates to provide past convictions and turns down an application in case of refusal. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

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;
- 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 a 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 subjected 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 collected. 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 life cycle 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,
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs are reviewed periodically and reasonably 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 providing 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 events are logged in a manner to ensure that only authorized trusted access is able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.
The events are protected in a manner to keep them readable in the time of their storage.
The 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, 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 invoked 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 then GlobalSign CA determines whether to suspend GlobalSign CA operations until the problem is solved duly informing the 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 lifecycle management events, including:-

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle 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 Issuer CA keys.

GlobalSign CA and Subscriber Certificate lifecycle management events, including:-

- Certificate requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts;
- 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 the GlobalSign CA

Time stamping:-

- 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 LRAs (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 to 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 Time-Stamping of Records

If a time stamping service is used to date the records, then it has to respect the requirements defined in section 6.8. Irrespective of time stamping 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 respects the security requirements defined in section 5.3.

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 co-ordinated 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 line with section 6.3.2. Certificate subject information may also be modified and certificate profiles may be altered to highlight new best practices. 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 in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan.
GlobalSign CA personnel that own a trusted role and operational role are specially trained to operate according to procedures defined in the Disaster Recovery plan for the most sensitive activities.
If a 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, the 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, however the signature keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate certificates status information according to GlobalSign CAs disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In case a GlobalSign CA signature key is compromised, lost, destroyed or suspected to be compromised:

- GlobalSign CA, after investigation of the problem decides whether 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;

- o 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 (with a rate of 99.95% availability excluding planned maintenance operations).

5.8 CA or RA Termination

In the event of termination of an 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
- Archive 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;
- Use secure means to notify customers and software platform providers 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 video taped/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 16 (sixteen) digit password. The first 8 (eight) digits are system generated and advised to the subscriber during the enrolment process and the subscriber decides the remaining 8 (eight). For SMIME certificates this is again achieved through the use of PCKS#12 (.pfx) files containing Private Keys and Certificates encrypted by a 8 (eight) digit subscriber selected password.
GlobalSign CA guarantees the integrity of any 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 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 line 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 as 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 digital 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 via the Subscriber in the form of a chain of certificates or via a repository operated by the 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 recommended timelines and best practice in the choice of size of its Keys for Root CAs, Issuing CAs and only signs end entity certificates following best practice. The same practice is contractually obligated to any Sub Issuing CAs in the TrustedRoot program outside of the direct control of the GlobalSign CA.

The following Key sizes and hashing algorithms are used for Root Certificates, Issuing Certificates and End Entity Certificates and CRL/OCSP certificate status responders in line with CABForum Base Requirements and Extended Validation Processes:-

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

Where possible the entire certificate chain and any certificate status responses use the same level of security and cryptography. Exceptions due to cross-certified certificates are acceptable.

Existing certificates with an unsuitable cryptographic strength are replaced in sufficient time as to protect relying parties, Subscribers and Issuing CAs.

6.1.6 Public Key Parameters Generation and Quality Checking

GlobalSign CA generates keys in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of 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 enrolment 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). Root Key material 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 line with the obligations that are presented in the form of a Subscriber Agreement or Terms of use Agreement.

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 Cryptographic 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	Certificate Term.
Root Certificates[3] -	20 years	30 years
TPM Root Certificates -	30 years	40 years
Issuing CA -	11 years	15 years
PersonalSign 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 Certificates -	No stipulation	5 years
EV SSL Certificates -	No stipulation	27 months
Time Stamping Certificates -	11 years	11 years
CA for AATL Certificates -	No stipulation	5 years
PDF Signing Certificates -	No stipulation	5 years
TrustedRoot	No stipulation	10 years
NAESB Certificates -	2 years	2 years

GlobalSign CA complies with the CABForum Minimum Guidelines for Publically Trusted SSL Certificates with respect to the maximum validity, therefore reducing the effective available certificate term.

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 shareholder who is a person in Trusted Role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issue 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.

---

[3] *2048 bit keys Generated prior to 2003 using RSA may be used for 25 years due to limited usage due to key size restrictions within hardware, root stores and operating systems.*

6.5 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;
- 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 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the 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 developed are developed in a controlled environment, and the development process 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 is 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 obtained from sources authorized by local policy. GlobalSign CA hardware and software are scanned for malicious code on first use and periodically thereafter;
- Hardware and software updates are purchased or developed in the same manner as original equipment; and be 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 Life Cycle 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 implements appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of 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 & 3 non-authenticated NTP source clocks to establish the correct time:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates;
- 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 CDS Subscriber digital IDs have the ability to include a trusted time stamp 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. Time-stamping 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 Time-stamping certificate in compliance to 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 have the ability to include a trusted time stamp 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. Time-stamping 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 Time-stamping 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 digital certificates in compliance with X.509 Version 3

7.1.2 Certificate Extensions

GlobalSign CA issues digital 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 digital 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 digital 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 digital certificates with name constraints where necessary and mark as critical where necessary as part of the TrustedRoot 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 digital certificates with a Policy Qualifier and suitable text to aid relying parties determine 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

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. TrustedRoot CAs that are not constrained by dNSNameConstraints are audited for compliance to one or both of the following standards:-

- AICPA/CICA WebTrust for Certification Authorities Version 1.0
- AICPA/CICA WebTrust for Extended Validation

8.1 Frequency and Circumstances of Assessment

GlobalSign CA maintains its compliance to the AICPA standards mentioned above via an independent auditor on an annual basis. The audit covers all of GlobalSign CA's activities.

8.2 Identity/Qualifications of Assessor

An audit of GlobalSign CA is performed by Ernst & Young as a Qualified Auditor that possess 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 Scheme;
- 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 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 the 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 highlighted to the GlobalSign CA policy authority.

8.6 Communications of Results

Results of the Audit are reported to the CPS 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 or renewal. GlobalSign CA does not charge for re-issuance (re-key during the lifetime of the certificate). Fees and any associated terms and conditions are made clear to Applicants both by the enrolment 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 CAs certificate status infrastructure.

9.1.4 Fees for Other Services

GlobalSign CA may charge for other additional services such as Time Stamping.

9.1.5 Refund Policy

GlobalSign CA offers a refund policy to Subscribers 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 2 million US dollars in coverage and Errors and Omissions / Professional Liability insurance with a policy limit of at least 5 million US dollars 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 https://www.globalsign.com/repository

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classed as being Confidential Information and therefore are subject to reasonable care and attention by GlobalSign CA staff including Vetting Operators 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), Business Continuity Plans (BCP)
- 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 line with a Privacy Policy published on GlobalSign CA's web site 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 digital 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 line 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 https://www.globalsign.com/repository

9.4.5 Notice and Consent to Use Private Information

Personal Information obtained from Applicants during the application and enrolment process is deemed private and permission is therefore required from the Applicant to allow the use of such information. GlobalSign CA incorporates the relevant provisions within an appropriate Subscriber Agreement including any additional information 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 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 the 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:-

- The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
- All Application Software Suppliers with whom the Root 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.

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 including:-

- **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 Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if GlobalSign CA and Subscriber are Affiliated, 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 CABForum Baseline Requirements (See section 4.9.1)

GlobalSign CA represents and Warrants that for NAESB PersonalSign Pro certificates

- GlobalSign CA has issued, and will manage, the certificate in accordance with the NAESB WEQ PKI Standards.
- GlobalSign has complied with all requirements in this 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 WEQ PKI standards.

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
- All translated material provided by the RA is accurate

9.6.3 Subscriber Representations and Warranties

Unless otherwise stated in this CPS, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with GlobalSign CA.
- Ensuring that the public key submitted to the GlobalSign CA correctly corresponds to the private key used.
- Accepting all terms and conditions in any subscriber agreement, GlobalSign CP and associated policies published in the GlobalSign CA repository.
- Refraining from tampering with an issued certificate.
- Using certificates only for legal and authorised purposes in accordance with this CPS.
- Notifying the GlobalSign CA or RA of any changes in the information submitted.
- Ceasing to use a certificate if any featured information becomes invalid.
- Ceasing to use a certificate when it becomes invalid.
- Removing a certificate when invalid from any applications and/or devices they have been installed on.
- Using a certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.
- Submit accurate and complete information to GlobalSign CA in accordance with the requirements of this CPS particularly with regards to registration.
- Only use the key pair for digital signatures and in accordance with any other limitations notified to the subscriber according to this CPS or any Trusted Root CA Chaining agreement.
- Exercise absolute care to avoid unauthorized use of its private key.
- Use a key length and algorithm as indicated in this CPS.

- Notify GlobalSign CAs without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The subscriber's private key has been lost, stolen, potentially compromised; or
    - Control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code or Pass Phrase)
      or
    - Inaccuracy or changes to the certificate content, as notified to the Subscriber.

The Subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and GlobalSign CA must designate the usage of a trustworthy device as well as the choice of organizational context.

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 Business Practice Standard WEQ-012, 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 these Business Practice Standards.
Each subscriber organization acknowledges their understanding of the following obligations to the WEQ 012 v3.0 PKI standard through GlobalSign CA as follows:-

Each End Entity organization shall certify to their certification entity that they have reviewed and acknowledge the following Business Practice Standard WEQ-012.

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

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

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

C. End Entity has evaluated each of its selected certificate authority's Certification Practices Statement in light of those industry standards as identified by the certificate 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 the GlobalSign as required by GlobalSign's Certification Practices Statement necessary for the GlobalSign to issue Certificates to the End Entity for use in securing electronic communications.
- Comply with all obligations required and stipulated by the by GlobalSign in this certification practices agreement, 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.

9.6.3.2 North American Energy Standards Board (NAESB) Relying Parties

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

- the Certificate was issued by GlobalSign, a registered Authorized Certification Authority;
- the entire Certificate validation/trust chain to the 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 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

GlobalSign CA does not warrant that:-

- The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CPS and in a Warranty Policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.8 Limitations of Liability

IN NO EVENT, EXCEPT FOR FRAUD OR WILLFUL MISCONDUCT, SHALL GLOBALSIGN CA BE LIABLE FOR ANY INDIRECT, INCIDENTAL 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, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EXCEPT FOR DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THIS CPS) ON THE VERIFIED INFORMATION ON THE MOMENT OF ISSUANCE OF THE CERTIFICATE TILL AN AMOUNT AS INDICATED BY THE WARRANTY COMMUNICATION DOCUMENT IN THE APPROPRIATE LEGAL REPOSITORY OF GLOBALSIGN CA'S WEB SITE. GLOBALSIGN CA WILL NOT BE LIABLE IN THIS CASE IF THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILLFUL MISCONDUCT OF THE APPLICANT. GLOBALSIGN CA WILL NOT BE LIABLE IN THIS CASE IF THE USER HAS NOT RESPECTED HIS OBLIGATIONS MENTIONED IN THIS CPS.

9.9 Indemnities

9.9.1 Indemnification by GlobalSign CA

GlobalSign CA shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by the Application Software Vendor 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 Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the Application Software Vendor'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 TrustedRoot 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, an End - User License 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 notice of the opposite is communicated by the GlobalSign CA on its web site or repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10.3 Effect of Termination and Survival

GlobalSign CA will communicate the conditions and effect of this CPS termination via their 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 the GlobalSign CA must be addressed to: legal@globalsign.com or by post to the GlobalSign CA in the address mentioned 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) parties agree to notify GlobalSign CA of the dispute with a view 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 by 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 resting 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 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 CP 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 digital 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 the 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 the GlobalSign CA, subscribers and relying parties) agree to conform to 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 Survival

The obligations and restrictions contained under section "Legal Conditions" survive the termination of this CPS.

9.16.3 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.

9.16.4 Assignment

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

9.16.5 Severability

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

9.16.6 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