

GlobalSign
Statement

Certification

Practice

Author: Andreas Mitrakas

Date: 13/03/2006

Version: v.5.1

Table of Contents

Document History.....	1
History 2	
Acknowledgments	3
1. Introduction.....	4
1.1 Overview	5
1.2 GlobalSign Certificate types	7
1.2.1 Personal Certificates	7
1.2.2 Server Certificates	7
1.2.3 Object Publishing Certificates.....	8
1.2.4 Acceptable Subscriber Names	8
1.2.5 Registration procedures	8
1.3 PersonalSign 1 Demo	8
1.3.1 General.....	8
1.3.2 Assurance level	9
1.3.3 Individuals.....	9
1.3.4 Content.....	9
1.3.5 Submitted documents to identify the applicant.....	10
1.3.6 Time to confirm submitted data	10
1.3.7 Issuing procedure	10
1.3.8 Limited Warranty.....	10
1.3.9 Relevant GlobalSign Legal Documents	10
1.4 PersonalSign 2	11
1.4.1 General.....	11
1.4.2 Assurance Level	11
1.4.3 Individuals.....	11
1.4.4 Content.....	12
1.4.5 Documents Submitted to Identify the Applicant.....	12
1.4.6 Time to Confirm Submitted Data	12
1.4.7 Issuing Procedure	12
1.4.8 Limited Warranty.....	12
1.4.9 Relevant GlobalSign Documents.....	12
1.5 PersonalSign 2 Pro	13
1.5.1 General.....	13
1.5.2 Individuals.....	13
1.5.3 Content.....	14
1.5.4 Documents Submitted to Identify the Applicant.....	14
1.5.5 Time to Confirm Submitted Data	14
1.5.6 Issuing Procedure	14
1.5.7 Limited Warranty.....	15
1.5.8 Relevant GlobalSign Documents.....	15
1.6 PersonalSign 3	15
1.6.1 General.....	15
1.6.2 Individuals.....	15
1.6.3 Content.....	16
1.6.4 Documents Submitted to Identify the Applicant.....	16
1.6.5 Time to Confirm Submitted Data	16
1.6.6 Issuing Procedure	16
1.6.7 Limited Warranty.....	17
1.6.8 Relevant GlobalSign Documents.....	17
1.7 PersonalSign 3 Pro	17
1.7.1 General.....	17
1.7.2 Individuals.....	17
1.7.3 Content.....	18

1.7.4	Documents Submitted to Identify the Applicant.....	18
1.7.5	Time to Confirm Submitted Data	18
1.7.6	Issuing Procedure	18
1.7.7	Limited Warranty.....	19
1.7.8	Relevant GlobalSign Documents.....	19
1.8	ServerSign.....	19
1.8.1	General.....	19
1.8.2	Business Entities.....	19
1.8.3	Content.....	20
1.8.4	Certificate Profile.....	20
1.8.5	Documents Submitted to Identify the Applicant.....	20
1.8.6	Time to Confirm Submitted Data	20
1.8.7	Issuing Procedure	20
1.8.8	Limited Warranty.....	21
1.8.9	Relevant Globalsign Documents	21
1.9	SureServer	21
1.9.1	General.....	21
1.9.2	Business Entities.....	21
1.9.3	Content.....	21
1.9.4	Information Submitted to Identify the Applicant.....	22
1.9.5	Time to Confirm Submitted Data	22
1.9.6	Issuing Procedure	22
1.9.7	Limited Warranty.....	22
1.9.8	Relevant Globalsign Documents	22
1.10	SureServer EDU	23
1.10.1	General.....	23
1.10.2	Business Entities.....	23
1.10.3	Content.....	23
1.10.4	Information Submitted to Identify the Applicant.....	23
1.10.5	Time to Confirm Submitted Data	24
1.10.6	Issuing Procedure	24
1.10.7	Limited Warranty.....	24
1.10.8	Relevant Globalsign Documents	24
1.11	ObjectSign.....	24
1.11.1	General.....	24
1.11.2	Business Entities.....	25
1.11.3	Content.....	25
1.11.4	Documents Submitted to Identify the Applicant.....	25
1.11.5	Time to Confirm Submitted Data	25
1.11.6	Issuing Procedure	25
1.11.7	Limited Warranty.....	26
1.11.8	Relevant GlobalSign Legal Documents	26
1.12	HyperSign.....	26
1.12.1	General.....	26
1.12.2	Business Entities.....	27
1.12.3	Content.....	27
1.12.4	Documents Submitted to Identify the Applicant.....	27
1.12.5	Time to Confirm Submitted Data	27
1.12.6	Issuing Procedure	27
1.12.7	Disclaimer.....	28
1.12.8	Limited Warranty.....	28
1.12.9	Relevant GlobalSign Documents.....	28
1.12.10	Approval	28
1.12.11	Applicant profile	28
1.13	Certificate usages	28
1.14	Document Name and Identification.....	29
1.15	PKI participants.....	30

1.15.1	GlobalSign Certification Authority	30
1.15.2	GlobalSign Registration Authorities	32
1.15.3	Subscribers.....	33
1.15.4	Subjects.....	33
1.15.5	Certificate Applicants	34
1.15.6	Relying Parties.....	34
1.16	Certificate use	34
1.16.1	Appropriate certificate usage.....	34
1.16.2	Prohibited certificate usage	34
1.16.3	Certificate extensions.....	35
1.16.4	Critical Extensions	35
1.17	Policy Administration.....	35
1.17.1	Scope	35
1.17.2	GlobalSign Policy Management Authority.....	35
1.17.3	Acceptance of Updated Versions of the CPS.....	36
1.17.4	Version management and denoting changes.....	36
1.18	Definitions and acronyms.....	36
2.	Publication and Repository Responsibilities.....	37
2.1	Access control on repositories.....	37
3.	Identification and Authentication.....	38
3.1	Naming	38
3.2	Initial Identity Validation	38
3.3	Subscriber registration process	39
3.3.1	Documents used for subscriber registration.....	39
3.3.2	Data needed for subscriber registration.....	41
3.3.3	Pseudonyms.....	42
3.3.4	Records for subscriber registration	42
3.4	Identification and Authentication for Revocation Requests.....	43
4.	Certificate Life-Cycle Operational Requirements	44
4.1	Certificate Application	44
4.2	Certificate Application Processing	44
4.3	Certificate Issuance	45
4.4	Certificate generation.....	45
4.5	Certificate Acceptance	45
4.6	Key Pair and Certificate Usage	45
4.6.1	Subscriber	46
4.6.2	Relying party.....	47
4.7	Certificate Renewal	47
4.8	Certificate Revocation and Suspension	47
4.8.1	Term and Termination of Suspension and Revocation.....	48
4.9	Certificate Status Services	48
4.10	End of Subscription.....	48
5.	Management, Operational, And Physical Controls.....	49
5.1	Physical Security Controls.....	49
5.2	Procedural Controls	49
5.3	Personnel Security Controls.....	50
5.3.1	Qualifications, Experience, Clearances	50
5.3.2	Background Checks and Clearance Procedures.....	50
5.3.3	Training Requirements and Procedures	50
5.3.4	Retraining Period and Retraining Procedures.....	50
5.3.5	Job Rotation	50
5.3.6	Sanctions Against Personnel.....	50
5.3.7	Controls of independent contractors.....	50
5.3.8	Documentation for initial training and retraining	50
5.4	Audit Logging Procedures	51
5.5	Records Archival.....	51
5.5.1	Types of records	52

5.5.2	Retention period	52
5.5.3	Protection of archive	52
5.5.4	Archive Collection	52
5.5.5	Procedures to obtain and verify archive information.....	52
5.6	Compromise and Disaster Recovery	52
5.7	CA or RA Termination	53
6.	Technical Security Controls.....	54
6.1	Key Pair Generation and Installation	54
6.1.1	GlobalSign CA Private Key Generation Process.....	54
6.1.2	GlobalSign CA Key Generation	54
6.2	Key Pair re-generation and re-installation	54
6.2.1	GlobalSign CA Key Generation Devices.....	55
6.2.2	GlobalSign CA Private Key Storage	55
6.2.3	GlobalSign CA Public Key Distribution.....	55
6.2.4	GlobalSign CA Private Key Destruction.....	55
6.3	Private Key Protection and Cryptographic Module Engineering Controls.....	56
6.4	Other Aspects of Key Pair Management.....	56
6.4.1	Computing resources, software, and/or data are corrupted.....	56
6.4.2	CA public key revocation.....	56
6.4.3	CA private key is compromised.....	56
6.5	Activation Data.....	56
6.6	Computer Security Controls	56
6.7	Life Cycle Security Controls	57
6.8	Network Security Controls.....	57
6.9	Time-stamping.....	57
7.	Certificate and CRL Profiles	58
7.1	Certificate Profile.....	58
7.2	CRL Profile	58
7.3	OCSP Profile	58
8.	Compliance Audit And Other Assessment	59
8.1	Compliance Audit And Other Assessment	59
8.1.1	Audit process conditions	59
9.	Other Business and Legal Matters	61
9.1	Fees	61
9.1.1	Refund policy.....	61
9.2	Financial Responsibility.....	61
9.3	Confidentiality of Business Information.....	61
9.3.1	Disclosure Conditions	62
9.4	Privacy of Personal Information.....	62
9.5	Intellectual Property Rights	63
9.6	Representations and Warranties	63
9.6.1	Subscriber Obligations	63
9.6.2	Relying Party Obligations.....	64
9.6.3	Subscriber Liability Towards Relying Parties	65
9.6.4	GlobalSign CA Repository and Web site Conditions.....	65
9.6.5	GlobalSign CA Obligations.....	66
9.6.6	Registration Authority Obligations	67
9.6.7	Information incorporated by reference into a digital certificate.....	67
9.6.8	Pointers to incorporate by reference.....	67
9.7	Disclaimers of Warranties	67
9.7.1	Limitation for Other Warranties.....	67
9.7.2	Exclusion of Certain Elements of Damages.....	68
9.8	Limitations of Liability	68
9.9	Indemnities	68
9.9.1	Indemnity.....	68
9.10	Term and Termination	69
9.11	Individual notices and communications with participants.....	69

9.12	Amendments.....	69
9.13	Dispute Resolution Procedures	69
9.13.1	Arbitration	69
9.14	Governing Law.....	70
9.15	Compliance with Applicable Law	70
9.16	Miscellaneous Provisions	70
9.16.1	Survival.....	70
9.16.2	Severability	70
10.	List of definitions	71
11.	List of acronyms.....	75

Document History

Document Change Control

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
	13/03/06	Johan Sys	Added SureServer EDU

History

Changes in v.5.1 (Publication Date: 13 March 2006) with respect to v.5.0

- Added SureServer EDU 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:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3039: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- ETSI TS 101 862: Qualified certificate profile.
- 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

1. Introduction

This Certification Practice Statement (CPS) of the GlobalSign Certification Authority (hereinafter, GlobalSign CA) applies to the services of the GlobalSign CA that are associated with the issuance of and management of digital certificates. Digital certificates can be used to create or rely upon electronic signatures. This CPS can be found on the GlobalSign CA repository at: <https://www.globalsign.net/repository>. This CPS may be updated from time to time.

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". This CPS is a certificate policy in broad sense and meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format. 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 in the implementation of the certificate management services of the GlobalSign CA. These sections have been removed from this document. Where necessary additional information is presented as subsections added to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability of the GlobalSign CA with other third party CAs and provides relying parties with advance notice on the practices and procedures of the GlobalSign CA. Additional assertions on standards used in this CPS can be found under section "Acknowledgements".

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by the GlobalSign CA.

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

GlobalSign NV
attn. Legal Practices,
Ubicenter,
Philipssite 5
B-3001 Leuven,
Belgium.
Tel: + 32 (0)16 287123
Fax: + 32 (0) 16 287404
Email: legal@globalsign.net
URL: www.globalsign.net

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 certificate types. More information can be obtained from <https://www.globalsign.net/repository>.

This CPS is final and binding between GlobalSign NV/SA, a company under public law, with registered office at Ubicenter, Philipssite 5, B-3001 Leuven, VAT Registration Number BE 459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (Hereinafter referred to as "GlobalSign")

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the GlobalSign CA.

For subscribers this CPS becomes effective and binding by accepting a subscriber agreement. For relying parties this CPS becomes binding by merely addressing a certificate related request on a GlobalSign certificate to a GlobalSign directory. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.

1.1 Overview

This CPS applies to the specific domain of the GlobalSign CA. The purpose of this CPS is to present the GlobalSign practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to GlobalSign'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 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 through discreet CA issuing Client end entity certificates. The certificate types addressed in this CPS are the following:

PersonalSign 1 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 3	A personal certificate of high assurance
PersonalSign 3 Pro	A personal certificate of high assurance with reference to professional context
ServerSign	A certificate to authenticate web servers
SureServer	A certificate to authenticate web servers
SureServer EDU	A certificate to authenticate web servers
ObjectSign	A certificate to authenticate data objects
HyperSign	A certificate for web servers with high encryption level
RootSign/Omniroot	A certificate for CAs that enter the GlobalSign hierarchy

GlobalSign 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 authenticate and trust other certification authorities.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of GlobalSign certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved including the GlobalSign CA, GlobalSign RA, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application providers etc.

This CPS describes the requirements to issue, manage and use certificates issued by the GlobalSign CA under a managed Brand Root. As a top root CA, GlobalSign manages a hierarchy of certificates according to publicised practices to be found under www.globalsign.net/repository.

A GlobalSign Certificate Policy (CP) complements this CPS. The purpose of the GlobalSign CP is to state the "what is to be adhered to" and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services. Such level is generally defined by the entity wishing to ensure a level of trust by managing the life cycle of digital certificates. The GlobalSign

CP addresses the requirements of the entire application domain of GlobalSign certificates focusing on top root certificates and not just the end-entity certificate area.

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 prevailing processes, procedures and overall prevailing conditions that the Certification Authority uses in creating and maintaining the certificates that it manages. In addition to the CP and CPS GlobalSign maintains a range of adjacent documented policies which include but are not limited to addressing such issues as:

- Business continuity
- Security policy
- Personnel policies
- Key management policies
- Registration procedures
- Etc.

Additionally, other pertinent documents include:

- The GlobalSign Limited Warranty Policy that addresses issues on insurance.
- The GlobalSign Data Protection Policy on the protection of personal data
- The GlobalSign Consumer Protection Policy regarding the protection of consumers
- The GlobalSign Certificate Policy that addresses the trust objectives for the domain of the GlobalSign top root.

A subscriber or relying party of a GlobalSign CA certificate must refer to the GlobalSign CPS in order to establish Trust on a certificate issued by the GlobalSign Root 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 GlobalSign certificate hierarchy, including the Top Root CA and operational roots, which can be established on the basis of the assertions of this CPS.

A full list of accreditation(s), and recognition of service is available upon request.

GlobalSign is additionally committed to implementing a high-level international and European standards prevailing in the area of digital certificates pursuant to the European Directive 99/93/EC implemented in Belgium by the Law of 9 July 2001. This CPS meets the requirements of ETSI TS 102 042 medium level.

The exact name of the GlobalSign CA certificates that makes use of this CPS is:

- GlobalSign Root CA
- GTE Cybertrust Global root

They are called collectively the GlobalSign CA Root.

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data electronically. By means of a digital certificate, GlobalSign 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 provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such entity uses. An entity on this instance might include an end use, another certification authority, as it might be required under the circumstances. GlobalSign makes available general-purpose digital certificates that can be used for non-repudiation and authentication. The use of these certificates can be further limited to a specific business or contractual context or transaction level according a warranty policy or other limitations imposed by the applications that certificates are used in.

This CPS is maintained by the GlobalSign CA, which is the issuing authority of certificates in the GlobalSign Public Key Infrastructure. In a certificate management environment based on Public Key Infrastructure (PKI), an Issuing Authority is the entity that manages a Trust hierarchy from which all end user certificates inherit Trust.

This CPS governs the issuance of certificates during the application period of the GlobalSign CA Roots. An application period is for example, the time during which a certain CA may issue GlobalSign CA certificates. The application period is indicated in the certificate issued to the appropriate Root by a hierarchically superior CA within the GlobalSign hierarchy.

This CPS is made available on-line in the Repository of the issuing CA under <https://www.globalsign.net/repository>.

The GlobalSign CA accepts comments regarding this CPS addressed to the address mentioned above in the Introduction of this document.

1.2 GlobalSign Certificate types

This part describes the public GlobalSign products.

1.2.1 Personal Certificates

GlobalSign offers several types of certificates for individuals, that can be used for web browsing, secure e-mail, inter organisational communications, access to personal financial information, online Internet transactions.:

- **PersonalSign Demo:** provides only an unambiguous e-mail address within the GlobalSign repository while GlobalSign performs no authentication of the identity of the applicant. PersonalSign Demo certificates are meant for test and demonstration purposes only and they are valid for one month or one year.
- **PersonalSign 2:** provides a limited identity authentication by requiring a signed copy of an identity element. These personal digital certificates for browsers can be used for most low-value/low risk commercial transactions like online purchases. They are valid for one, two or three years.
- **PersonalSign 2 Pro:** provides a limited identity authentication by requiring a signed copy of an identity proof. PersonalSign 2 Pro certificates require professional context affiliation. These personal digital certificates for browsers can be used for most low-value/low risk commercial transactions like online purchases. They are valid for one, two or three years.
- **PersonalSign 3:** provides a high level of identity assurance by requiring that the applicant appear personally before a Registration Authority to prove its identity. These certificates can be used for high-value/high risk commercial transactions such as electronic banking. They are valid for one, two or three years.
- **PersonalSign 3 Pro:** provides a high level of identity assurance by requiring that the applicant appears personally before a Registration Authority to prove its identity. PersonalSign 3 Pro certificates require professional context affiliation. These certificates can be used for high-value/high risk commercial transactions such as electronic banking. They are valid for one, two or three years.

1.2.2 Server Certificates

GlobalSign offers several types of certificates for servers, that can be used for web based transactions, such as the following:

- **ServerSign:** ServerSign is meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based

businesses engaging in commercial and financial transactions. The identity of the ServerSign-holder is fully authenticated by GlobalSign.

- **HyperSign:** is a server-level certificate, which "enhances" SSL technology to deliver strong (128-bit) encryption in an Internet browsing session. HyperSign addresses the need for additional security in especially sensitive electronic transactions or communications while, subject to US export rules, they are currently available to banks, financial institutions, insurance companies, health and medical organisations, online merchants and overseas subsidiaries of US companies.
- **SureServer:** SureServer is meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in commercial and financial transactions. The identity of the SureServer-holder is fully authenticated by GlobalSign.
- **SureServer EDU:** SureServer is meant for entities within the education and research space that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based education and research institutes. The identity of the SureServer-holder is fully authenticated by GlobalSign.

1.2.3 Object Publishing Certificates

GlobalSign offers one type of object certificate software objects such as the following:

- **ObjectSign** ensures the identity of an entity that distributes software or software object such as applets etc. on the Internet, and guarantees the integrity of the software being distributed as well, utilizing Microsoft Authenticode or Netscape's ObjectSigning standards. ObjectSign assures relying parties of the integrity of a n object and verifies the identity of the sender of a software object to ensure that the certified software object originates from a trusted source.

1.2.4 Acceptable Subscriber Names

For publication in its certificates GlobalSign accepts subscriber names that are meaningful and can be authenticated as required for each product type or class.

1.2.4.1 Pseudonyms

For certain types of products GlobalSign may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law or a following a reasoned and legitimate request.

1.2.5 Registration procedures

For all types of certificates GlobalSign reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.

1.3 PersonalSign 1 Demo

1.3.1 General

PersonalSign Demo certificates are issued to natural persons (individuals) only.

PersonalSign 1 Demo certificates confirm that a user's e-mail address forms an unambiguous subject name within the GlobalSign repository.

PersonalSign Demo certificates are communicated electronically to subscribers and added to its set of available certificates.

They are typically used for Web browsing and personal E-mail, to establish continuity in the sequence of communications (providing assurances that follow-up communications are from the same user). They are not intended for commercial use where proof of identity is required and should not be relied upon for such uses.

PersonalSign 1 Demo certificates are intended for test purposes only.

PersonalSign 1 Demo certificates can be distributed as an introduction to digital certificates, for applications that do not require authentication of the communicating parties and for encryption of the e-mail communications.

PersonalSign 1 Demo certificates validity period is 30 days or one year.

Although PersonalSign 1 Demo certificates are not essentially technically different from other classes of GlobalSign personal certificates, as there is no verification process, the identity of the applicant cannot be warranted.

1.3.2 Assurance level

PersonalSign Demo certificates do not facilitate the authentication of the identity of the subscriber as they merely represent a simple check of the non-ambiguity of the e-mail address within the GlobalSign repository.

The subscriber's E-mail address contained in a PersonalSign 1 Demo certificate consists of non-verified subscriber information for the accuracy of which GlobalSign carries no responsibility.

1.3.3 Individuals

The procedure for a certificate request can be made as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.3.4 Content

Typical of information published in a PersonalSign 1 demo certificate includes the following elements.

- Subscriber's e-mail address

- Subscriber's public key
- Issuing certification authority (GlobalSign):
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.3.5 Submitted documents to identify the applicant

No registration documents are necessary for PersonalSign 1 Demo certificates.

1.3.6 Time to confirm submitted data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

1.3.7 Issuing procedure

The following steps describe the milestones to issue a PersonalSign 1 Demo certificate:

- 1 The applicant fills out the online registration form, as part of the online request
- 2 The applicant accepts the online subscriber agreement
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
- 4 The public key and the online request are sent to GlobalSign automatically.
- 5 GlobalSign authorises the issuance of a certificate
- 6 GlobalSign sends e-mail to the applicant with a URL that permits the applicant to retrieve the certificate.
- 7 GlobalSign publishes the issued certificate in an on line database.
- 8 Renewal: not allowed
- 9 Revocation: allowed but remains at GlobalSign's discretion

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.3.8 Limited Warranty

GlobalSign accepts no liability and offers no insurance for issuing PersonalSign 1 Demo certificates.

1.3.9 Relevant GlobalSign Legal Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Privacy Policy
- 4 Consumer Policy
- 5 Insurance Policy

1.4 PersonalSign 2

1.4.1 General

PersonalSign 2 certificates are intended for communications and transactions that require a minimum verification of the identity.

PersonalSign 2 certificates can be distributed for communications and transactions with a low value and little risk with a need to authenticate the communicating parties and encrypt the exchange of communications.

PersonalSign 2 certificates validity period is one, two or three years.

PersonalSign 2 certificates are issued to natural persons (individuals) only.

PersonalSign 2 applicant verification is undertaken by a registration authority by using a copy of an identity proof.

PersonalSign 2 certificates are issued primarily for low value and low risk personal communications and purposes.

Records retention period **does not** fulfil professional records requirements according to the Laws of Belgium.

1.4.2 Assurance Level

PersonalSign 2 certificates may provide reasonable, but not foolproof, assurance of a subscriber's identity, based on an automated on-line process that compares the applicant's name, address, and other personal information on the certificate application against a signed identity proof.

Although GlobalSign's PersonalSign 2 on-line identification process is a high level method of authenticating a certificate applicant's identity, it does not require the applicant's personal appearance before a registration authority.

1.4.3 Individuals:

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.

1.4.4 Content

Typical information published on a PersonalSign 2 certificate includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign):
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.4.5 Documents Submitted to Identify the Applicant

The applicant must submit to a GlobalSign Registration Authority a signed copy of an identification document such as an identity card, driver's licence or passport. The applicant's signature must be preceded by the date of signing and the phrase 'I have read and I approved the subscriber agreement'

1.4.6 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm the certificate application information and issue a digital certificate within reasonable time frames. For PersonalSign 2 verification 1 to 3 working days might be needed.

1.4.7 Issuing Procedure

The following steps describe the milestones in the procedure to issue a PersonalSign 2 certificate:

- 1 The applicant fills out the outline registration form: e-mail address, common name, country code, verification method, billing information as part of the online request.
- 2 The applicant accepts online subscriber agreement.
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.).
- 4 The public key and online request are sent to GlobalSign.
- 5 GlobalSign verifies by checking copy of verification method and payment.
- 6 RA may positively verify the applicant.
- 7 GlobalSign may issue the certificate to the applicant.
- 8 GlobalSign publishes the issued certificate in on line database.
- 9 Renewal: allowed.
- 10 Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.4.8 Limited Warranty

GlobalSign accepts liability up to 2500 EURO per damage caused by a false identity in a PersonalSign 2 certificate issued according to the CPS

1.4.9 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy
- 4 Consumer Policy
- 5 Limited WarrantyPolicy

1.5 PersonalSign 2 Pro

This part describes the specific requirements for PersonalSign 2 Pro certificates.

1.5.1 General

PersonalSign 2 Pro certificates are intended for certain communications and transactions that require a minimum verification of the identity.

PersonalSign 2 Pro certificates can be distributed for communications and transactions with a low value and little risk with a need to authenticate the communicating parties and encrypt the exchanged communications.

PersonalSign 2 Pro certificates validity period is one, two or three years years.

PersonalSign 2 Pro certificates are issued to natural persons (individuals) within their professional context only.

PersonalSign 2 Pro applicant identification is done by a registration authority by using a copy of an identity proof.

PersonalSign 2 Pro certificates are typically used primarily for intra-organisational and inter-organisational E-mail; small, "low-risk" transactions; personal/individual E-mail; password replacement; software validation; online purchases and on-line subscription services.

Records retention period **fulfils** professional records requirements according to the Laws of Belgium.

1.5.2 Individuals

A certificate request can be made by the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to the applicant's device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.5.3 Content

Typical content of information published on a PersonalSign 2 Pro certificate includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's professional organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.5.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

Employees are required to submit the articles of association of their employer and obtain confirmation of their employment relationship.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a Self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional proof of identity in support of the verification of the applicant.

1.5.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For PersonalSign 2 Pro verification 1 to 5 working days might be needed.

1.5.6 Issuing Procedure

The issuing procedure for a PersonalSign 2 certificate is as follows:

- 1 The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
- 2 The applicant accepts the on line subscriber agreement.
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.).
- 4 The public key and the online request are sent to GlobalSign automatically
- 5 Applicant must mail to a RA copies of identity, articles of association, professional context and payment information.
- 6 RA may positively verify the applicant.
- 7 GlobalSign may issue the certificate to the applicant.
- 8 GlobalSign publishes the issued certificate in on line database.
- 9 Renewal: allowed.
- 10 Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.5.7 Limited Warranty

GlobalSign accepts liability up to 2500 EURO per damage caused by a false identity in a PersonalSign 2 Pro certificate issued according to the CPS.

1.5.8 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy
- 4 Consumer Policy
- 5 Limited Warranty Policy

1.6 PersonalSign 3

1.6.1 General

PersonalSign 3 certificates are intended for high value commercial transactions such as electronic banking and contract execution.

PersonalSign 3 certificates offer a high level of identity assurance requiring personal presence before a registration authority.

PersonalSign 3 certificates are issued to natural persons (individuals) without a professional context.

PersonalSign 3 certificates validity period is one, two or three years.

PersonalSign 3 certificates are issued primarily for medium risk **personal communications** and usages.

Records retention period **does not** fulfil professional records requirements according to the Laws of Belgium.

1.6.2 Individuals:

A certificate request can be made as follows:

On-line: Via the Web (<https>). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such

additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or information to be included in the certificate.

1.6.3 Content

Typical content of information published on a PersonalSign 3 certificate includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.6.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit to a GlobalSign Registration Authority in person a signed registration form, a signed subscriber agreement and a copy of identity proof.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

1.6.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For PersonalSign 3 verification 1 to 5 working days might be required.

1.6.6 Issuing Procedure

The issuance procedure for a PersonalSign 3 certificate is as follows:

- 1 The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
- 2 The applicant accepts the on line subscriber agreement.
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
- 4 The public key and the online request are sent to GlobalSign automatically
- 5 GlobalSign verifies by personal appearance before a LRA or RA and checking identity elements of the applicant as well as payment. **NB. Personal presence may occur prior to the time of the application**
- 6 RA may positively verify the applicant.
- 7 GlobalSign may issue the certificate to the applicant.
- 8 GlobalSign publishes the issued certificate in on line database.
- 9 Renewal: allowed.
- 10 Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.6.7 Limited Warranty

GlobalSign accepts liability up to 37500 EURO per damage caused by a false identity in a PersonalSign 3 certificate issued within the terms of this CPS.

1.6.8 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy
- 4 Consumer Policy
- 5 Insurance Policy

1.7 PersonalSign 3 Pro

1.7.1 General

PersonalSign 3 Pro certificates are intended for high value commercial transactions such as electronic banking and contract execution.

PersonalSign 3 Pro certificates offer a high level of identity assurance requiring personal presence before a registration authority.

PersonalSign 3 Pro certificates are issued to natural persons (individuals) **within their professional context only**.

PersonalSign 3 Pro certificates validity period is one two or three years.

PersonalSign 3 Pro certificates are issued primarily for professional usages.

Records retention period **meets** professional records requirements according to the Laws of Belgium.

1.7.2 Individuals

A certificate request can be made as follows:

On-line: Via the Web (<https>). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant

must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.7.3 Content

Typical content of information published on a PersonalSign 3 Pro certificate includes the following elements:

- Applicant's e-mail address
- Applicant's name
- Applicant's public key
- Applicant's professional organisation or affiliation
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.7.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit in person to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

For an employee it is required to submit the articles of association of its employer and confirmation by a legal representative of such organisation.

For a self-employed person that works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For self-employed persons belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional identification proof in support of the verification of the applicant.

1.7.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For PersonalSign 3 Pro verification 1 to 5 working days might be needed.

1.7.6 Issuing Procedure

The following steps describe the milestones in the issuance of a PersonalSign 3 Pro certificate:

- 1 The applicant submits online the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
- 2 The applicant accepts the on line subscriber agreement.
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
- 4 The public key and the online request are sent to GlobalSign automatically
- 5 GlobalSign verifies by personal appearance before a LRA or RA and checking articles of association, proof of professional context and payment. **NB. Personal presence may occur prior to the time of the application.**
- 6 RA may positively verify the applicant.

- 7 GlobalSign may issue the certificate to the applicant.
- 8 GlobalSign publishes the issued certificate in on line database.
- 9 Renewal: allowed.
- 10 Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.7.7 Limited Warranty

GlobalSign accepts liability up to 37500 EURO per damage caused by a false identity in a PersonalSign 3 Pro certificate issued according to the CPS.

1.7.8 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Data Protection Policy
- 4 Consumer Policy
- 5 Limited WarrantyPolicy

1.8 ServerSign

1.8.1 General

ServerSign certificates are meant for secure communication with for example a web-site through an SSL or TLS link.

The applicant is an organisation that has an Internet Server such as a website. Server certificates are used to assure the Internet Server's identity to the visitor and to assure a confidential communication with the Internet Server.

ServerSign certificates validity period is one, two or three years according to the choice of the applicant.

ServerSign certificates are issued to legal entities and self employed professionals registered with a professional organisation.

The period retention for records **meets** professional records requirements of the Laws of Belgium.

1.8.2 Business Entities

A certificate request can be made in the following ways:

On-line: Via the Web (<https>). The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity of the Internet Server, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that

GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of the identity of the Internet Server, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.8.3 Content

Typical information published on a ServerSign certificate includes the following elements

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.8.4 Certificate Profile

1.8.5 Documents Submitted to Identify the Applicant

The applicant must submit to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation.

1.8.6 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For ServerSign verification 1 to 5 working days might be required.

1.8.7 Issuing Procedure

The issuing procedure for a a ServerSign certificate is as follows:

- 1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
- 2 The applicant follows the on line registration procedure.
- 3 The applicant submits the required information including organizational information, technical contact, server information, payment information.
- 4 The applicant accepts the on line subscriber agreement.
- 5 Data is sent with certificate request to GlobalSign automatically.
- 6 GlobalSign verifies the submitted information by checking organisational, payment and any other information as it sees fit. This may also include checks in third party databases or resources.
- 7 GlobalSign may positively verify the applicant.
- 8 GlobalSign may issue the certificate to the applicant.
- 9 GlobalSign publishes the issued certificate in online database
- 10 Renewal: allowed
- 11 Revocation: allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.8.8 Limited Warranty

GlobalSign accepts liability up to 37500 EURO per loss due to a false identity in a certificate issued following the CPS.

1.8.9 Relevant Globalsign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.net/repository:

- 1 CPS
- 2 Subscriber Agreement
- 3 Limited Warranty Policy

1.9 SureServer

1.9.1 General

SureServer certificates are meant for secure communication with for example a web-site through an SSL or TLS link.

The applicant is an organisation that has an Internet Server such as a website. Server certificates are used to assure the Internet Server's identity to the visitor and to assure a confidential communication with the Internet Server.

SureServer certificates validity period is one year, two years or three years.

SureServer certificates are issued to legal entities and self employed professionals registered with a professional organisation.

The period retention for records fulfils professional records requirements of the Laws of the United States.

1.9.2 Business Entities

A certificate request can be made in the following ways:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity of the Internet Server, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

1.9.3 Content

Typical information published on a SureServer certificate includes the following elements

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign Omniroot)
- GlobalSign electronic signature
- Type of algorithm

- Validity period of the digital certificate
- Serial number of the digital certificate

1.9.4 Information Submitted to Identify the Applicant

The applicant must provide business and contact details to GlobalSign and underwrite those by click-through process. GlobalSign has the right to request a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation if it deems necessary. Independent verification through consulting industry or other database with telephone confirmation will be performed.

1.9.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For SureServer verification 1 to 5 working days might be required.

1.9.6 Issuing Procedure

The issuing procedure for a SureServer certificate is as follows:

- 1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
- 2 The applicant follows the on line registration procedure.
- 3 The applicant submits the required information including organizational information, technical contact, server information, payment information.
- 4 The applicant accepts by click-through the on line subscriber agreement.
- 5 Data is sent with certificate request to GlobalSign automatically.
- 6 GlobalSign verifies the submitted information by checking organisational, payment and any other information as it sees fit. This may also include checks in third party databases or resources and independent verification through telephone.
- 7 GlobalSign may positively verify the applicant.
- 8 GlobalSign may issue the certificate to the applicant.
- 9 GlobalSign publishes the issued certificate in online database
- 10 Renewal: allowed
- 11 Revocation: allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.9.7 Limited Warranty

GlobalSign accepts liability up to 100000 Dollars per loss due to a false identity in a SureServer certificate issued following the CPS.

1.9.8 Relevant Globalsign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.net/repository:

- 1 GlobalSign CPS
- 2 Subscriber Agreement

1.10 SureServer EDU

1.10.1 General

SureServer EDU certificates are meant for secure communication with for example a web-site through an SSL or TLS link.

The applicant is an organisation within the educational or research environment that has an Internet Server such as a website. Server certificates are used to assure the Internet Server's identity to the visitor and to assure a confidential communication with the Internet Server.

SureServer EDU certificates validity period is one year, two years or three years.

SureServer EDU certificates are issued to entities and self employed professionals registered with a professional organisation which is operating in the educational or research space.

The period retention for records fulfils professional records requirements of the Laws of the United States.

1.10.2 Business Entities

A certificate request can be made in the following ways:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity of the Internet Server, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

1.10.3 Content

Typical information published on a SureServer EDU certificate includes the following elements

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign Omniroot)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.10.4 Information Submitted to Identify the Applicant

The applicant must provide business and contact details to GlobalSign and underwrite those by click-through process. GlobalSign has the right to request a signed registration form, a signed subscriber agreement, the articles of association of the applying organisation and proof of the applying organisation belonging to the educational or research market if it deems necessary. Independent verification through consulting industry or other database with telephone confirmation will be performed.

1.10.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For SureServer EDU verification 1 to 5 working days might be required.

1.10.6 Issuing Procedure

The issuing procedure for a SureServer EDU certificate is as follows:

- 1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
- 2 The applicant follows the on line registration procedure.
- 3 The applicant submits the required information including organizational information, technical contact, server information and if required payment information.
- 4 The applicant accepts by click-through the on line subscriber agreement.
- 5 Data is sent with certificate request to GlobalSign automatically.
- 6 GlobalSign verifies the submitted information by checking organisational and any other information as it sees fit. This may also include checks in third party databases or resources and independent verification through telephone.
- 7 GlobalSign may positively verify the applicant.
- 8 GlobalSign may issue the certificate to the applicant.
- 9 GlobalSign publishes the issued certificate in online database
- 10 Renewal: allowed
- 11 Revocation: allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.10.7 Limited Warranty

SureServer EDU is exempt from GlobalSign's limited warranty program. To the extent permitted by law, SureServer warranty is limited to 1 Euro for any case of proven damages to a subscriber.

1.10.8 Relevant Globalsign Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.net/repository:

- 1 GlobalSign CPS
- 2 Subscriber Agreement

1.11 ObjectSign

1.11.1 General

ObjectSign certificates are used for the signing of software objects, such as software packages or applets.

ObjectSign certificates validity period is one, two or three years.

ObjectSign certificates are issued to legal entities and self-employed professionals.

The period retention for records **meets** professional records requirements according to the Laws of Belgium.

1.11.2 Business Entities

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends the certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of information to be included in the certificate.

1.11.3 Content

Typical information published on a ObjectSign certificate includes the following elements:

- Applicant's e-mail address
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.11.4 Documents Submitted to Identify the Applicant

The applicant must submit to a GlobalSign Registration Authority a copy of identity proof such as an identity card, driver's license or passport and the articles of association of the applying organisation (if applicable).

1.11.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within the reasonable time frames. For ObjectSign verification might require 1 to 5 working days.

1.11.6 Issuing Procedure

Below following the steps to issue an ObjectSign certificate:

- 1 The applicant fills out online the registration form: e-mail address, organizational info, common name, country code, payment info
- 2 The applicant accepts the online subscriber agreement
- 3 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
- 4 The public key and online request are sent to GlobalSign automatically

5 GlobalSign verifies the submitted information by checking organisational, payment and any other information as it sees fit also through third party databases or resources. This may also include checks in third party databases or resources and independent verification through telephone.

6 GlobalSign may positively verify the applicant.

7 GlobalSign may issue the certificate to the applicant.

8 GlobalSign publishes the issued certificate in an online database

9 Renewal: allowed

10 Revocation: allowed

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.11.7 Limited Warranty

GlobalSign accepts liability up to a maximum of 37500 EURO per loss due to a false identity in an ObjectSign certificate issued within the terms of the CPS.

1.11.8 Relevant GlobalSign Legal Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

1 CPS

2 Subscriber Agreement

3 Limited Warranty Policy

4 Data Protection Policy (if applicable)

1.12 HyperSign

1.12.1 General

HyperSign certificates are meant for secure communication with a web site through an SSL link that allows for 128-bit encryption with certain types of older web-browsers using Server Gated Crypto (SGC) technology.

HyperSign certificates provide a high level of credibility for an organisational web site.

The period retention for records **meets** professional records requirements according to the Laws of Belgium.

HyperSign has a validity period of one year.

The applicant is an organisation that has a website and that is eligible to receive GlobalSign SGC server certificates under current U.S. policy on encryption export control as mentioned in the subscriber agreement that is available on <https://www.globalsign.net/repository>.

HyperSign certificates are currently available to:

- Banks
- Financial Institutions
- Banking and Financial Service Systems
- Insurance companies
- Health and Medical Organizations
- Online Merchants
- U.S. Subsidiaries

1.12.2 Business Entities

A certificate request can be made as follows:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link following a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign the additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.

E-mail: The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice on information to be included in the certificate.

1.12.3 Content

Typical information published in a HyperSign certificate includes the following:

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

1.12.4 Documents Submitted to Identify the Applicant

The applicant must submit to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation.

1.12.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For HyperSign verification might require 1 to 5 working days.

1.12.6 Issuing Procedure

The following steps describe the milestones in the issuing of a HyperSign 128 certificate:

- 1 The applicant proves its eligibility by electing the sector its organisation belongs to and submits server information.
- 2 The applicant creates a Certificate Signing Request (CSR) and a key pair using appropriate server software.
- 3 The applicant copies and paste its certificate signing request and submits it to GlobalSign.
- 4 The applicant confirms the information included in its certificate-signing request.
- 5 The applicant submits the required information including organizational information, technical contact, server information, and payment information.
- 6 The applicant verifies the organizational and payment information.
- 7 The applicant accepts the on line subscriber agreement.

- 8 Data is sent with certificate request to GlobalSign automatically.
 - 9 GlobalSign verifies the submitted information by checking organizational, payment and any other information at it sees fit also through third party databases or resources.
 - 10 GlobalSign may positively verify the applicant.
 - 11 GlobalSign may issue the certificate to the applicant.
 - 12 GlobalSign publishes the issued certificate in its online database.
 - 13 Renewal: allowed.
 - 14 Revocation: allowed.
- GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.12.7 Disclaimer

GlobalSign reserves its right to issue SGC certificates only as it sees appropriate taking into account all circumstances related to the issuing of a SGC certificate.

GlobalSign disclaims any and all liability for damages, including indirect and consequential damages, from refusing to issue a SGC certificate as requested by any party.

1.12.8 Limited Warranty

GlobalSign accepts liability up to 37500 EURO per loss due to a false identity in a certificate issued following the CPS.

1.12.9 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on <https://www.globalsign.net/repository>:

- 1 CPS
- 2 Subscriber Agreement
- 3 Limited WarrantyPolicy

1.12.10 Approval

GlobalSign has been granted approval to issue SGC server certificates (i.e. HyperSign) to certain classes of organizations for Microsoft Web Server Software, subject to export licenses issued by the United States Department of Commerce.

1.12.11 Applicant profile

Applicant represents that it is one of the following entities that are eligible to receive GlobalSign HyperSign certificates under current US policy on encryption export control.

1.13 Certificate usages

Certain limitations apply to the use of GlobalSign certificates. A GlobalSign certificate can only be used for purposes explicitly permitted as they are listed below:

Electronic signature: Electronic signature can only be used for specific electronic transactions that support electronic signing of electronic forms, electronic documents, electronic mail etc. The signature certificate is only warranted to produce electronic signatures in the context of applications that support digital certificates. To describe the function of an electronic signature, the term non-repudiation is often used. Certificates that are appropriate for electronic signature are the following:

PersonalSign 2: non repudiation of a transaction (medium level)

PersonalSign2 Pro: : non repudiation of the transaction by a party acting in an organisational context (medium level)

PersonalSign 3: non repudiation of the transaction (high level)

PersonalSign 3 Pro: non repudiation of the transaction by a party acting in an organisational context (high level)

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)
- PersonalSign2 Pro: authentication of a natural person within an organisational context (medium level)
- PersonalSign 3: authentication of a natural person (high level)
- PersonalSign 3 Pro: authentication of a natural person within an organisational context (high level)

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.

- ServerSign: authentication of a remote domain name and webservice and encryption of the communication channel.
- SureServer: authentication of a remote domain name and webservice and encryption of the communication channel.
- SureServer EDU: authentication of a remote domain name and webservice and encryption of the communication channel.
- ObjectSign: authentication of a data object.
- HyperSign: authentication of a remote domain name and webservice and encryption of the communication channel at a high level.

Confidentiality: All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality is required to assure the confidentiality of business and personal communications as well as for purposes of personal data protection and privacy.

Any other use of a digital certificate is forbidden. When using a digital certificate the functions of electronic signature (non repudiation) and authentication (digital signature) are permitted together with the same certificate. The different terms used i.e. electronic signature as opposed to non-repudiation and authentication as opposed to digital signature relate to the different terminology in the IETF and the vocabulary adopted in the legal framework in the European Union manifested by the Directive 1999/93/EC on a Community framework on electronic signatures. .

1.14 Document Name and Identification

GlobalSign ensures compliance of its certificates with the requirements and assertions of this CPS. This CPS implements the policy requirements defined in ETSI TS 101 042. This CPS is a certificate policy according to the terminology used in ETSI TS 101 042, because it demonstrates how GlobalSign meets the requirements for issuing certificates.

GlobalSign assures of its conformance with the identified certificate policy requirements.

1.15 PKI participants

The GlobalSign CA makes its services available to GlobalSign subscribers. These subscribers include without limitation entities that use certificates for the purposes of:

- Authentication (digital signature)
- Electronic signature (non-repudiation)
- Encryption

A subject is a natural person that successfully applies for a certificate. Any other uses of certificates are restricted. Certificates can be used for any public purposes. As “public” this CPS considers any use that takes place among subscribers who are not restricted to uses governed by voluntary agreements under private law among participants.

NB. Under the scope of this policy general-purpose uses associated with services made available by the Belgian government are allowed. GlobalSign reserves its right to evaluate uses within various application environments that it does not specifically prohibit. Subscribers and relying parties are hereby notified to contact GlobalSign before applying for or using a certificate in an application domain, which mandates proprietary or non-public requirements with a view to ensure the functionality of certificates.

1.15.1 GlobalSign Certification Authority

A Certification Authority, such as GlobalSign, is an organisation that issues digital certificates to be used in public or private domains, within a business framework, a transactions context etc. A certification authority is also referred to as the Issuing Authority to denote the purpose of issuing certificates at the request of an RA.

The GlobalSign CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates. The GlobalSign CA is a Policy Authority with regard to issuing GlobalSign CA certificates. The GlobalSign CA has ultimate control over the lifecycle and management of the GlobalSign CA Root and any subsequent root belonging to its hierarchy.

The GlobalSign CA ensures the availability of all services pertaining to the management of certificates under the GlobalSign CA Root, including without limitation the issuing, revocation, status verification of a certificate, as they may become available or required in specific applications. The GlobalSign CA also manages a core online registration system for all certificate types, issued under the GlobalSign CA Root.

Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of functions associated with the revoked and/or suspended certificates. Publication is manifested by including a revoked or suspended certificate in a certificate revocation list that is published in an online directory. Issued certificates also appear on directories of issued certificates. The GlobalSign CA operates such directories.

The domain of responsibility of the GlobalSign CA's comprises of the overall management of the certificate lifecycle including the following actions:

- Issuance
- Suspension
- Unsuspension
- Revocation
- Renewal
- Status validation

- Directory service

Some of the tasks attributed to the certificate lifecycle are delegated to selected GlobalSign RAs that operate on the basis of a service agreement with GlobalSign.

1.15.1.1 GlobalSign outsource agent

Through an outsource agent GlobalSign operates a secure facility in order to deliver CA services including the issuance, suspension, revocation, renewal and status validation of GlobalSign CA certificates. The GlobalSign outsource agent operates a service to GlobalSign on the basis of a service agreement. The scope of the service is the support in certificate management. The GlobalSign outsource agent warrants designated services and service levels that meet those required by GlobalSign. The GlobalSign outsource agent carries out tasks associated with the administration of services and certificates on behalf of GlobalSign.

1.15.1.2 Roles of GlobalSign

GlobalSign operates under two discreet roles. Firstly, as a Trust Service Provider to deliver Trust Services to a user community, directly or through an agent. An agent in this case includes third party entities, called Registration Authorities (RAs) that operate under agreement with and within the conditions laid out by GlobalSign.

Secondly GlobalSign operates an international network of Trusted Third Parties (TTP's) sharing the GlobalSign procedures and using suitable brand name to issue high quality and highly trusted digital certificates to public and private entities. Such partners include GlobalSign accredited Certification Authorities and RAs that operate under an agreement with GlobalSign. This role is typically limited to the issuance of certificates to other certification authorities, which seek to inherit trust that is usually vested in the GlobalSign CA root and brand name.

The main activities of GlobalSign are to:

- Manage an international network of RAs, establishing the brand name of GlobalSign as a universal Trusted Third Party leveraging on in PKI technology.
- Manage the life cycle of digital certificates issued to end user entities as well as to other certification authorities and administrators within the GlobalSign domain.

The GlobalSign public certification services aim at supporting secure electronic commerce and on-line business services to address the business and personal requirements of the users of electronic signatures.

The Distinguished name of the issuer is further specified in section "Certificate Profile" of this CPS.

Responding to the need for secure electronic transactions among users and service providers in a global market place, GlobalSign published or documented practices support the GlobalSign infrastructure and to deliver high quality trust services to diverse user communities in Europe and the world. GlobalSign is a subsidiary of Cybertrust.

1.15.1.3 GlobalSign root and hierarchy

GlobalSign makes available to subscribers a dedicated root hierarchy to ensure the integrity of the end user certificate and the uniqueness of the resources made available for digital certificates. The GlobalSign CA manages a broader range of the GlobalSign trust network that includes roots that have been set up to fulfil specific purposes such as the issuance of end user certificates at levels defined by GlobalSign etc. as well as other participating CAs that take

advantage from GlobalSign's root, which is embedded in applications. The GlobalSign Certificate Policy addresses the Root level of the GlobalSign hierarchy.

The GlobalSign CA root has been used to certify each of the private keys of the subsequent third party CA roots. By validating the certificate of such a CA, trust vested in GlobalSign can also be extended to the certified third party CA root.

The roots that are addressed under this CPS include:

- PersonalSign 1
- PersonalSign 2
- PersonalSign2 Pro
- PersonalSign 3
- PersonalSign 3 Pro
- ServerSign
- ObjectSign
- HyperSign
- SureServer
- SureServer EDU

1.15.2 GlobalSign Registration Authorities

The GlobalSign CA reaches its subscribers through a designated Registration Authorities. An RA requests the issuance, suspension and revocation of a certificate under this CPS.

An RA submits the necessary data for the generation and revocation of the certificates to the CA.

A GlobalSign RA interacts with the subscriber to deliver public certificate management services to the end-user. A GlobalSign RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to GlobalSign CA certification services.
- Attends all stages of the identification of subscribers as assigned by the GlobalSign CA according to the type of certificates they issue.
- Uses official, notarised or otherwise authorised documents to evaluate a subscriber application.
- Following approval of an application, notify the GlobalSign CA to issue a certificate.
- Initiates the process to suspend, or unsuspend or revoke a certificate and request a certificate revocation from the GlobalSign CA Root.

The GlobalSign RA acts locally on approval and authorisation by the GlobalSign CA. The GlobalSign RA acts in accordance with the approved practices and procedures of the GlobalSign CA including this CPS and documented GlobalSign RA procedures.

Sometimes to grant a specific certificate type, GlobalSign RAs might rely on certificates issued by third party certification authorities or other third party databases and sources of information. Belgian electronic identity cards are such a source of authoritative subscriber information. Relying Parties are hereby prompted to seek specific information by referring to the appropriate certificate policies prevailing in managing specific certificate types issued under the GlobalSign Root.

If successful, the evaluation is followed by the issuance of the certificate to the applicant organisation.

Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of RAs.

1.15.3 Subscribers

Subscribers of GlobalSign services are natural or legal persons that successfully apply for a certificate. Subscribers use electronic signature services within the domain of the GlobalSign. Subscribers are parties that:

- Set the framework of providing certification services with the GlobalSign CA to the benefit of the subject mentioned in a certificate.
- Have ultimate authority over the private key corresponding to the public key that is listed in a subject certificate.

Natural persons that are subscribers typically hold a valid identification document, such as an identity card, passport or equivalent, which is used as credential in order to issue electronic certificates.

Legal persons are identified on the basis of the published by-laws and appointment of Director as well as the subsequent government gazette (e.g. Staatsblad/Moniteur Belge in Belgium etc.) or other third party databases. Self-employed 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 that require accessing GlobalSign network resources.

Subscribers are also sometimes operational or legal owners of signature creation devices that are issued with for the purpose of generating a key pair and storing a certificate.

It is expected that a subscriber organisation has an employment or service agreement or otherwise a pre-existing contract relationship with GlobalSign authorising it to carry out a specific function within the scope of an application that uses GlobalSign certificate services. Granting a certificate to a subscriber organisation is only permitted pursuant to such an agreement between GlobalSign and the subscribing end entity.

1.15.4 Subjects

Subjects of GlobalSign CA certificates services are natural persons only that are themselves subscribers or are associated with a subscriber. Subjects use electronic signature services under authorisation of and within the domain that is designated by the subscriber (if applicable). Subjects are parties that:

- Apply for a certificate.
- Are identified in a certificate.
- Hold the private key corresponding to the public key that is listed in a subscriber certificate.

A subject enrolls with the GlobalSign RA or a Service Provider that requires it to use a certificate within the designated service. A subject nominates a named Certificate Applicant also called a Subscriber, to apply for a certificate. A certificate applicant can be any natural person acting on behalf of the subject.

Natural persons can be listed as subjects of the following certificates:

- PersonalSign 2
- PersonalSign2 Pro
- PersonalSign 3
- PersonalSign 3 Pro

Legal persons or self-employed professionals can be listed as subjects of the following certificates:

- ServerSign
- SureServer
- SureServer EDU
- ObjectSign
- HyperSign

1.15.5 Certificate Applicants

A certificate applicant is a party wishing to become a subscriber of a certificate. A certificate applicant is a party designated by the subject to act on the subject's behalf in:

- Applying for a certificate.
- Agreeing with and accepting the CA's subscriber agreement.

The applicant may be:

- The same as the subject itself, where this is a named individual.
- An individual employed by the subject.
- An individual employed by a contractor, or sub-contractor acting upon explicit authorisation.

1.15.6 Relying Parties

Relying parties are natural 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. For example, the GlobalSign operators that receive signed requests from GlobalSign CA subjects are relying parties of the GlobalSign certificates.

To verify the validity of a digital certificate, relying parties must always refer to GlobalSign CA revocation information, currently a Certificate Revocation List (CRL). Certificate validation takes place prior to relying on information featured in a certificate. Alternatively, relying parties may refer to an automated response by using the OCSP protocol where available. Relying parties meet specific obligations as described in this CPS.

1.16 Certificate use

Certain limitations apply to the use of GlobalSign CA certificates.

1.16.1 Appropriate certificate usage

Certificates issued under the GlobalSign CA can be used for public domain transactions that require:

- Non-repudiation and
- Authentication
- Confidentiality

Additional uses are specifically designated once they become available to end entities. Unauthorised use of GlobalSign certificates may result in an annulment of warranties offered by the GlobalSign CA to subscribers and relying parties of GlobalSign certificates.

1.16.2 Prohibited certificate usage

End entity 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.

GlobalSign certificates are not authorised for use within Closed Groups unless such Groups have notified GlobalSign thereof and GlobalSign has consented to it. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the Limited Warranty Policy.

1.16.3 Certificate extensions

GlobalSign issues certificates that contain extensions defined by the X.509 v.3 standard other standards as well as any other formats including those used by Microsoft and Netscape.

GlobalSign uses certain constraints and extensions for its public PKI services as per the definition of the International Standards Organisation (ISO). Such constraints and extensions may limit the role and position of a CA or subscriber certificate so that such subscribers can be identified under varying roles.

As key usage extension limits the technical purposes for which a public key listed in a certificate may be used. GlobalSign's own certificates may contain a key usage extension that limits the functionality of a key to only signing certificates, certificate revocation lists, and other data.

A certificate policy extension limits the usage of a certificate to the requirements of a business or a legal context. GlobalSign pro-actively supports and participates in the proliferation of industry, government or other certificate policies for its public certificates as it sees appropriate.

1.16.4 Critical Extensions

GlobalSign 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 for 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.

1.17 Policy Administration

The GlobalSign CA is a top root authority (also known as trust anchor) that manages certificates services within its own domain. The GlobalSign CA might also interact with or seek recognition by third party certification authorities.

The Policy Managing Authority of the GlobalSign CA manages this GlobalSign CPS. The GlobalSign CA registers, observes the maintenance, and interprets this CPS. The GlobalSign CA makes available the operational conditions prevailing in the life-cycle management of certificates issued under the GlobalSign CA root. The operational conditions for each root are publicised in this CPS.

1.17.1 Scope

In an effort to invoke credibility and Trust in the publicised GlobalSign CPS and to better correspond to accreditation and legal requirements, GlobalSign may make revisions and updates to its policies as it sees fit or required by the 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 the CP and/or CPS.

1.17.2 GlobalSign Policy Management Authority

New versions and publicized updates of GlobalSign policies are approved by the GlobalSign Policy Management Authority. The GlobalSign Policy Management Authority in its present organisational structure comprises members as indicated below:

- At least one member of the management of GlobalSign.

- At least two authorised agents directly involved in the drafting and development of GlobalSign practices and policies.

The Management member chairs the GlobalSign Policy Management Authority ex officio.

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

1.17.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the GlobalSign Policy Management Authority that CPS is published in the GlobalSign online Repository at <https://www.globalsign.net/repository>.

GlobalSign publishes a notice of such updates on its public web site at <https://www.globalsign.net>. 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 GlobalSign 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 may submit objections to policy changes. Relying parties that are not subscribers do not have the right to submit objections and any such submissions will be regarded as never received.

GlobalSign publishes on its web site at least the two latest versions of its CPS.

1.17.3.1 Changes with notification

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

1.17.4 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

1.18 Definitions and acronyms

A list of definitions can be found at the end of this CPS.

2. Publication and Repository Responsibilities

GlobalSign publishes information about the digital certificates that it issues in an online publicly accessible repository. GlobalSign reserves its right to publish certificate status information on third party repositories.

GlobalSign retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CPS. GlobalSign reserves its right to make available and publish information on its policies by any appropriate means within the GlobalSign repository.

All parties who are associated with the issuance, use or management of GlobalSign certificates are hereby notified that GlobalSign may publish submitted information on publicly accessible directories in association with the provision of electronic certificate status information.

GlobalSign refrains from making publicly available certain elements of documents including security controls, procedures, internal security policies etc. However these elements are disclosed in audits associated with formal accreditation schemes that GlobalSign adheres to, such as Web Trust for CAs.

2.1 Access control on repositories

While GlobalSign 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.

3. Identification and Authentication

GlobalSign operates RAs that verify and authenticate the identity and/or other attributes of an end-user certificate applicant for a certificate.

Prior to requesting the CA to issue a certificate, GlobalSign RAs verify the identity of applicants of a certificate.

GlobalSign RAs maintain appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

GlobalSign RAs authenticate the requests of parties wishing to revoke certificates under this policy.

3.1 Naming

To identify a subscriber, the GlobalSign CA follows and the GlobalSign RAs apply certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names, RFC-822 names or X.400 names. The GlobalSign CA issues certificates to applicants that submit a documented application containing a verifiable name.

3.2 Initial Identity Validation

The identification of the applicant for a certificate is carried out according to a documented procedure to be implemented by the GlobalSign RAs.

For the identification and authentication procedures of the initial subscriber registration GlobalSign takes the following steps:

- The natural person identified in the subject field must demonstrate possession of the private key corresponding to the public key presented to the GlobalSign CA. The subject itself or its designated representative must demonstrate this.
- GlobalSign RAs might rely on such resources as third party databases to identify and authenticate natural persons applying for a certificate.

For the identification and authentication of appropriately authorised third party agents applying for a GlobalSign certificate controls include the following:

- Controlling physical identification documents such as an identity card or passport issued by a designated authority in the country of origin of the applicant.
- Authenticating the identity of the applicant based on other documentation or credentials provided.
- Requesting an applicant to physically appear before a GlobalSign RA prior to issuing a certificate.
- Requesting a third party agent or his/her principal (e.g. a GlobalSign contractor) to produce evidence with regard to the relationship between GlobalSign and the third party agent (e.g. an outsource contract etc.).

A GlobalSign RA may refuse issuing a certificate to an applicant unless sufficient evidenced is produced with regard to the applicant's identity. If an application is rejected applicants may subsequently reapply.

To issue certificates, a GlobalSign RA endeavours to provide the applicant with sufficient credentials (enrolment URL, password) such that the enrolment process can then proceed online.

At GlobalSign's discretion any such credentials may be two-factor, communicated by independent channels using agreed and proven contact methods.

The identification of an applicant for a certificate is carried out according to a documented procedure to be implemented by the GlobalSign RAs.

3.3 Subscriber registration process

GlobalSign ensures that:

- Subscribers of certificates are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.

In particular:

- GlobalSign provides notice to the applicant through its web site at www.globalsign.net and the dedicated policy framework published on its repository at www.globalsign.net/repository.
- Before entering any contractual relationship with the subscriber, GlobalSign makes available a subscriber agreement, which the applicant must approve prior to placing a request with GlobalSign. This agreement can also be consulted in advance on GlobalSign's repository at www.globalsign.net/repository.
- GlobalSign's policy framework is limited under data protection and consumer protection laws and warranty, as explained in the GlobalSign CPS as well as GlobalSign's Limited Warranty framework.
- GlobalSign maintains documented contractual relationships with all third party registration authorities or outsourced agents it uses to deliver certificates.

3.3.1 Documents used for subscriber registration

GlobalSign or an authorized GlobalSign RA typically verifies by appropriate means and on the basis of a documented procedure, the identity and, if applicable, all specific attributes thereof of applicants of certificates.

Evidence on identity is checked against a natural person either directly or indirectly using means which provide equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation. Examples of evidence checked indirectly against a natural person is documentation presented for registration that was acquired as the result of an application requiring physical presence.

Evidence on identity of organizations is checked against documents presented to establish the existence of organizations or through independent verification through third-party databases. Submitted evidence may be in the form of either paper or electronic documentation.

Self-employed professionals that are eligible to be issued with certificates typically have to prove their identity as individuals as well as their professional registration.

Specific documents required include the following:

3.3.1.1 PersonalSign 1

No specific documented proof of identity is required

3.3.1.2 PersonalSign 2

The applicant must submit to a GlobalSign Registration Authority a signed copy of an identification document such as an identity card, driver's licence or passport.

3.3.1.3 PersonalSign 2 Pro

In all cases, the applicant must submit to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

Employees are required to submit the articles of association of their employer and obtain confirmation of their employment relationship.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional proof of identity in support of the verification of the applicant.

3.3.1.4 PersonalSign 3

In all cases, the applicant must submit to a GlobalSign Registration Authority in person a signed registration form, a signed subscriber agreement and a copy of identity proof.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.1.5 PersonalSign 3 Pro

In all cases, the applicant must submit to a GlobalSign Registration Authority in person a signed registration form, a signed subscriber agreement and the articles of association or proof of professional context and a copy of identity proof.

For an employee it is required to submit the articles of association of its employer and confirmation by a legal representative of such organisation.

For a self-employed person that works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For self-employed persons belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional identification proof in support of the verification of the applicant.

3.3.1.6 ServerSign

The applicant must submit to a GlobalSign Registration Authority a signed registration form a signed subscriber agreement and the articles of association of the applying organisation.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.1.7 SureServer

The applicant must submit to a GlobalSign Registration Authority a registration form and a subscriber agreement, both accepted and agreed to through a click-through acceptance process.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.1.8 SureServer EDU

The applicant must submit to a GlobalSign Registration Authority a registration form and a subscriber agreement, both accepted and agreed to through a click-through acceptance process.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.1.9 ObjectSign

The applicant must submit to a GlobalSign Registration Authority a copy of identity proof such as an identity card, driver's license or passport and the articles of association of the applying organisation (if applicable).

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.1.10 HyperSign

The applicant must submit to a GlobalSign Registration Authority a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation.

GlobalSign may prescribe additional identification proof in support of the verification of the applicant's identity.

3.3.2 Data needed for subscriber registration

Where an applicant is natural person evidence shall be provided of the following data prior to accepting an application for a certificate:

- Full name (including surname and given names).
- Date of birth
- Place of birth
- A nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

Where the subscriber is a person who is identified in association with an organizational entity, proof will be produced in terms of:

- Full name (including surname and given names) of the subscriber.
- Date and place of birth, a nationally recognized identity number, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- Full name and legal status of the associated legal person or other organizational entity.

- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.

Where the subscriber is an organization, proof will be produced in terms of:

- Full name and legal status of the associated legal person of the organizational entity.
- Company registration number, VAT number or other attributes of the subscriber which may be used to, as far as possible, distinguish it from others with a similar same name.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that any natural person involved in the application process is associated with that organizational entity.

GlobalSign neither recommends nor encourages any specific choice of an end user product. Applicants and subscribers are entirely responsible to make the appropriate requests for the issuance of their certificates. Should support in identifying the features of each option be deemed necessary in order to make an informed selection, applicants are prompted to contact GlobalSign at: legal@globalsign.net.

3.3.3 Pseudonyms

GlobalSign may conditionally accept the use of pseudonyms in its certificates. GlobalSign reserves its right to refuse granting a pseudonym certificate following a reasonably justified application assessment. Reasons for rejecting a pseudonym application include but are not limited to a pseudonym being:

- Already is use
- Violating third party rights
- Constituting slander etc.

GlobalSign maintains documented records of a pseudonym application and application rejections.

Notice is hereby given that GlobalSign may disclose the real identity of the pseudonym certificate holder to any party, which can demonstrate a justified and legitimate interest to it.

The subscriber provides a physical address, or other attributes, which describe how the subscriber may be contacted.

GlobalSign reserves its right to insert names with pseudonyms in its certificates on a case-by-case basis. GlobalSign might make such designations in guidance documentation supplied to its RAs

3.3.4 Records for subscriber registration

GlobalSign records all information used to verify the subscriber identity, including any reference number on the documentation used for verification, and any limitations on the validity thereof.

GlobalSign maintains records of the executed subscriber agreement and any material or documents that support the application which also include but are not limited to:

- GlobalSign subscriber agreement as approved of, and executed by, the applicant.
- Consent to the keeping of a record by GlobalSign of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CPS in the case of the CA terminating its services.
- That information held in the certificate is correct and accurate.
- Full name of the subscriber.

- Date and place of birth, a nationally recognized identity number, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- A specifically designed attribute that uniquely identifies the applicant within the context of the GlobalSign CA.
- Proof of organization context where necessary.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subscriber is associated with that organizational entity.
- Any evidence produced in support of an application with a pseudonym.

The records identified above shall be kept for a period of no less than 5 years following the expiration of a certificate. A GlobalSign RA maintains such records. For organizational purposes a GlobalSign LRA may also maintain duplicates of these records for a shorter period of time.

3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests of its subject types (CA, RA, subscriber, and other participants) GlobalSign requires using an online authentication mechanism (e.g. digital certificate authentication, PIN etc.) and a request addressed to the GlobalSign CA or an RA.

4. Certificate Life-Cycle Operational Requirements

All entities within the GlobalSign domain including the RAs and subscribers or other participants have a continuous duty to inform the GlobalSign CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or gets revoked.

The GlobalSign CA issues, revokes or suspends certificates following an authenticated and duly signed request issued by a GlobalSign RA.

To carry out its tasks GlobalSign may use third party agents. GlobalSign assumes full responsibility and accountability for all acts or omissions of all third party agents it may use to deliver services associated with CA operations within the GlobalSign CA.

4.1 Certificate Application

A GlobalSign RA has the duty to provide the GlobalSign CA with accurate information on certificate requests it lodges on behalf of the end user applicants.

The GlobalSign CA acts upon request of an RA that has the authority to make a request to issue a certificate.

Subscribers undergo an enrolment process that requires:

- a. Filling out an application form.
- b. Generating a key pair, directly or through an agent.
- c. Delivering the generated public key corresponding to a private key to GlobalSign CA.
- d. Accepting the subscriber agreement.

In case of a subject that can be distinguished from a subscriber, then the above listed requirements (a) through to (d), are met by the subject; else, the subject's designated applicant meets them. The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the GlobalSign CA. The subscriber agreement incorporates by reference this CPS.

In general, an online enrolment process will be sufficient, only as explicitly permitted by GlobalSign. In all other cases credentials are requested, as appropriate, in a way that the exact identity of the applicant can reasonably be established. This includes a manually signed copy of the subscriber agreement, and a copy of identity card, or physical appearance before the RA.

4.2 Certificate Application Processing

A GlobalSign RA acts upon a certificate application to validate an applicant's identity. Subsequently, an RA either approves or rejects a certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

The RA acts upon a certificate application to validate an applicant's identity as foreseen in a documented procedure.

Pursuant to a certificate application the RA either approves or rejects a certificate application. If the application is approved the RA transmits the registration data to GlobalSign.

For rejected applications of certificate requests, the RA notes the reason for rejecting the application.

4.3 Certificate Issuance

The GlobalSign RA subsequently sends a certificate issuance request to the GlobalSign CA.

Requests from the RA are granted approval provided that they are validly made and they contain valid subscriber data, formatted according the GlobalSign CA specifications.

The GlobalSign CA verifies the identity of the GlobalSign RA on the basis of credentials presented (a special RA administrator certificate). The GlobalSign CA retains its right to reject the application, or any applicant for RA certificates.

Following issuance of the certificate, the GlobalSign CA delivers the issued certificate to the subscriber directly or through an agent.

4.4 Certificate generation

With reference to the issuance and renewal of certificates GlobalSign represents towards all parties that certificates are issued securely according to the conditions set below:

- The procedure to issue a certificate is securely linked to the associated registration, including the provision of any subscriber generated public key.
- The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket layer) links, especially when the applicant carries out CA/RA communications.
- The authentication of registrars is ensured through appropriate credentials issued to them.
- Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.
- GlobalSign verifies that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are ever used.
- GlobalSign accepts independent audits of its services and practices.

4.5 Certificate Acceptance

An issued GlobalSign CA certificate is deemed accepted by the subscriber when the RA confirms the acceptance of a certificate the CA issues.

Any objection to accepting an issued certificate must explicitly be notified to the GlobalSign CA. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The GlobalSign CA posts the issued certificate on a repository (X.500 or LDAP). The GlobalSign CA also reserves its right to notify the certificate issuance by the GlobalSign CA to other entities.

4.6 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

4.6.1 Subscriber

The obligations of the subscriber include the following ones:

4.6.1.1 Subscriber duties

Unless otherwise stated in this CPS, the duties of subscribers include the following:

1. Accepting all applicable terms and conditions in the CPS of GlobalSign published in the GlobalSign Repository.
2. Notifying the GlobalSign CA or a GlobalSign RA of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a GlobalSign certificate when it becomes invalid.
4. Using a GlobalSign certificate, as it may be reasonable under the circumstances.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
6. Using secure devices and products that provide appropriate protection to their keys.
7. For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
8. Refraining from submitting to GlobalSign or any GlobalSign directory any material that contains statements that violate any law or the rights of any party.
9. Request the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a GlobalSign CA certificate.
10. Refraining from tampering with a certificate.
11. Only using certificates for legal and authorised purposes in accordance with the CPS.

The Subscriber has all above stated duties towards the CA at all times. When the subscriber applies on behalf of a different named Subject certain duties can be mitigated to the Subject, which in return shall have to inform the Subscriber of any eventualities affecting the life cycle of a certificate. In such case of mitigation, duties 2, 3, 4, 5, 6, 8, 9 10, 11 above apply to the Subject and not to the Subscriber.

4.6.1.1.1 Certificate Life-Cycle Operational Requirements

Subscribers are hereby notified of their continuous duty to inform directly a GlobalSign RA of any and all changes in the information featured in a certificate during the validity period of such certificate or of any other fact that materially affects the validity of a certificate. This duty can be exercised either directly by the subscriber or through an agent.

GlobalSign issues, revokes or suspends certificates only at the request of the RA following a successful application of a certificate applicant.

4.6.1.2 Subscriber Duty Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CP, subscribers have a duty to refrain from any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

4.6.1.3 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The GlobalSign CA takes steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the GlobalSign CA Repositories and web site may result in terminating the relationship between the GlobalSign CA and the party.

4.6.2 Relying party

The duties of a relying party are as follows:

4.6.2.1 Relying party duties

A party relying on a GlobalSign certificate will:

- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign certificate by using certificate status information (e.g. a CRL or OCSP) published by GlobalSign, in accordance with the certificate path validation procedure and validate at least those certificate attributes that materially affect the relying party's own signature policy if available.
- Trust a GlobalSign CA certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign certificate, only as it may be reasonable under the circumstances.
- Trust a certificate only if it has not been suspended or revoked.
- Validate at least those certificate attributes that materially affect the relying party's own signature policy or practices.

4.6.2.2 GlobalSign CA Repository and Web site Conditions

Parties, including subscribers and relying parties, accessing the GlobalSign CA Repository and web site agree with the provisions of this CPS and any other conditions of use that the GlobalSign CA may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided:

- Obtaining information as a result of the search for a digital certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Validating the status of a digital certificate before encrypting data using the public key included in a certificate
- Obtaining information published on the GlobalSign CA web site.

4.7 Certificate Renewal

Subscribers may request the renewal of GlobalSign certificates. To request the renewal of a GlobalSign certificate, an end user lodges an online request.

Requirements for renewal of certificates, where available, may vary from those originally required for subscribing to the service.

4.8 Certificate Revocation and Suspension

The identification of the subscriber who applies for a revocation or suspension of a certificate is carried out according to an internal documented procedure. This procedure is subject to auditing by authorised parties in compliance with the requirements set by accreditation schemes.

Subject to prior agreement with GlobalSign any GlobalSign RA may carry out the identification and authentication of holders seeking to revoke or suspend a certificate. To this effect an authenticated request is needed to initiate the procedure. The requesting party will have to be

authenticated as the subscriber of that certificate or at least as an authorised agent of the subscriber of the certificate.

An RA might further challenge the requesting party until its identity is sufficiently established and distinguished from others.

Revocation and suspension requests can also be placed directly to the GlobalSign RA at: GlobalSign, Philipssite 5, 3001, Leuven, Belgium or ra@globalsign.net.

Upon request from an RA, the GlobalSign CA suspends or revokes a digital certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject.
- The certificate's subject or their appointed subscriber has breached a material obligation under this CPS.
- The performance of a person's obligations under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.

The GlobalSign RA requests the suspension or revocation of a certificate promptly upon verifying the identity of the requesting party. Verification of the identity can be done through information elements featured in the identification data that the subscriber has submitted to the GlobalSign RA. Upon request by a GlobalSign RA, the GlobalSign CA takes prompt action to revoke the certificate.

4.8.1 Term and Termination of Suspension and Revocation

Suspension may last for a maximum of seven calendar days to establish the conditions that caused the request of suspension.

The GlobalSign CA publishes notices of suspended or revoked certificates in the GlobalSign CA repository. The GlobalSign CA may publish its suspended or revoked certificates in its CRL and additionally, by any other means as it sees fit.

4.9 Certificate Status Services

The GlobalSign CA makes available certificate status checking services including CRLs, OCSP where applicable, and appropriate Web interfaces.

CRL

A CRL lists all revoked and suspended certificates during the application period. CRLs are available from <http://www.globalsign.net/crl>.

A CRL is issued each 3 hours.

4.10 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

5. Management, Operational, And Physical Controls

This section describes non-technical security controls used by GlobalSign CA to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1 Physical Security Controls

The GlobalSign CA implements physical controls on its own, leased or rented premises.

The GlobalSign CA infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

The GlobalSign CA secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

The GlobalSign CA implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The GlobalSign CA implements a partial off-site backup.

The sites of the GlobalSign CA host the infrastructure to provide the GlobalSign CA services. The GlobalSign CA sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list, which is subject to audit.

5.2 Procedural Controls

The GlobalSign CA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The GlobalSign CA obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The GlobalSign CA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted members of the GlobalSign CA staff need to bring their respective and split knowledge in order to be able proceed with an ongoing operation.

The GlobalSign CA ensures that all actions with respect to the GlobalSign CA can be attributed to the system and the person of the CA that has performed the action.

The GlobalSign CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The GlobalSign CA Partners perform checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks are specifically directed towards. Background checks include:

- Misrepresentations by the candidate.
- Any other as it might be deemed necessary.

5.3.2 Background Checks and Clearance Procedures

The GlobalSign CA makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or self-declarations.

5.3.3 Training Requirements and Procedures

The GlobalSign CA makes available training for their personnel to carry out CA and RA functions.

5.3.4 Retraining Period and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation

Not applicable.

5.3.6 Sanctions Against Personnel

GlobalSign CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.7 Controls of independent contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as GlobalSign CA personnel.

5.3.8 Documentation for initial training and retraining

The GlobalSign CA, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment. GlobalSign CA implements the following controls:

GlobalSign CA audit records events that include but are not limited to

- Issuance of a certificate
- Revocation of a certificate
- Suspension of a certificate
- Publishing of a CRL

Audit trail records contain:

- The identification of the operation
- The data and time of the operation
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents that are required for audits include:

- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

GlobalSign CA ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of GlobalSign CA, the RA and designated auditors. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up.

Auditing events are not given log notice.

5.5 Records Archival

The GlobalSign CA keeps internal records of the following items:

- All certificates for a period of a minimum of 1 year after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 1 year after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 1 year following the revocation of a certificate.
- CRLs for a minimum of 1 year after expiration or revocation of a certificate.
- Support documents on the issuance of certificates for a period of 5 years after expiration of a certificate.

In specific GlobalSign maintains records for a period of 5 years for the following products:

- PersonalSign 2 Pro
- PersonalSign 3
- PersonalSign 3 Pro
- ServerSign
- ObjectSign
- SureServer
- SureServer EDU

GlobalSign CA keeps archives in a retrievable format.

GlobalSign CA ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of GlobalSign CA and the RA as appropriate.

5.5.1 Types of records

GlobalSign CA retains in a trustworthy manner records of GlobalSign CA digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

5.5.2 Retention period

GlobalSign CA retains in a trustworthy manner records of certificates for at least 1 year.

5.5.3 Protection of archive

Conditions for the protection of archives include:

Only the records administrator (member of staff assigned with the records retention duty) may view the archive:

- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

5.5.4 Archive Collection

The GlobalSign CA archive collection system is internal.

5.5.5 Procedures to obtain and verify archive information

To obtain and verify archive information GlobalSign CA maintains records under clear hierarchical control.

The GlobalSign CA retains records in electronic or in paper-based format. The GlobalSign CA may require RAs, subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic or in paper-based format or any other format that the GlobalSign CA may see fit.

The GlobalSign CA may revise record retention terms as it might be required in order to comply with accreditation schemes including WebTrust for CAs.

5.6 Compromise and Disaster Recovery

In a separate internal document, the GlobalSign CA documents applicable incident, compromise reporting and handling procedures. The GlobalSign CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The GlobalSign CA establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

A business continuity plan has been implemented to ensure business continuity following a natural or other disaster.

5.7 CA or RA Termination

Before terminating its CA activities, the GlobalSign CA will take steps to transfer to a designated organisation the following information at the GlobalSign CA's own costs:

- All information, data, documents, repositories, archives and audit trails pertaining to the GlobalSign CA.

6. Technical Security Controls

This section sets out the security measures taken by the GlobalSign CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

6.1 Key Pair Generation and Installation

The GlobalSign CA protects its private key(s) in accordance with this CPS. The GlobalSign CA uses private signing keys only for signing CRLs, and OCSP responses in accordance with the intended use of each of these keys.

The GlobalSign CA will refrain from using its private keys used within the GlobalSign CA in any way outside the scope of GlobalSign CA.

6.1.1 GlobalSign CA Private Key Generation Process

The GlobalSign CA uses a trustworthy process for the generation of its root private key according to a documented procedure. The GlobalSign CA distributes the secret shares of its private key(s).

6.1.1.1 GlobalSign CA Private Key Usage

The private keys of the GlobalSign CA are used to sign GlobalSign CA issued certificates, GlobalSign CA certification revocation lists and OCSP responses. Other usages are restricted.

6.1.1.2 GlobalSign CA Private Key Type

For the CA Root key it uses, the GlobalSign CA makes use of the RSA algorithm with a key length of either 1024 or 2048 bits and a validity period of at least 14 years.

For the operational CA keys it uses the GlobalSign CA makes use of the RSA algorithm with a key length of 1024 bits and a validity period of up to 7 years.

6.1.2 GlobalSign CA Key Generation

The GlobalSign CA securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of them. The GlobalSign CA implements and documents key generation procedures, in line with this CPS.

The GlobalSign key generation is carried out using an algorithm recognized as being fit for the purposes of certificates. GlobalSign uses RSA SHA-1.

The selected key length and algorithm for CA signing key is recognized as being fit for the purposes of certificates as issued by the CA..

6.2 Key Pair re-generation and re-installation

The GlobalSign CA decommissions and destroys keys used in the past as well as the active tamper-resistant devices and all backup or escrowed copies of its private keys.

6.2.1 GlobalSign CA Key Generation Devices

The generation of the private keys of the GlobalSign CA occurs within a secure cryptographic device.

6.2.1.1 GlobalSign CA Key Generation Controls

The generation of the private key of the GlobalSign CA requires the control of more than one appropriately authorised member of staff serving in trustworthy positions. This action entails dual control.

6.2.2 GlobalSign CA Private Key Storage

The GlobalSign CA uses a secure cryptographic device to store its private keys meeting the appropriate requirements of ISO.

When outside the signature-creation device the GlobalSign private signing key for a certificate is encrypted at all times.

6.2.2.1 GlobalSign CA Key Storage Controls

The storage of the private key of the GlobalSign CA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.2 GlobalSign CA Key Back Up

The GlobalSign CA's private keys are backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.3 Secret Sharing

The GlobalSign CA secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of private keys and provide for key recovery. The GlobalSign CA stores its own private keys in several tamper-resistant devices. This action entails dual control.

6.2.2.4 Acceptance of Secret Shares

A secret shareholder receives the secret share within a physical medium, such as a GlobalSign CA approved hardware cryptographic module..

6.2.3 GlobalSign CA Public Key Distribution

Public key distribution of GlobalSign's own public key takes place according to GlobalSign's own practices.

6.2.4 GlobalSign CA Private Key Destruction

GlobalSign CA private keys are destroyed by at least two trusted operatives present at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

Key destruction process is documented and associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

The GlobalSign CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements, which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

GlobalSign CA custodians are assigned with the task to activate and deactivate the private key. The key is then active for a defined time period.

The GlobalSign CA private keys can be destroyed at the end of their lifetimes.

6.4 Other Aspects of Key Pair Management

The GlobalSign CA archives its own public keys. The GlobalSign CA issues subscriber certificates with usage periods as indicated on such certificates.

6.4.1 Computing resources, software, and/or data are corrupted

The GlobalSign CA establishes the necessary measures to ensure full recovery of the service in case of a disaster, corrupted servers, software or data.

If resources or services are not retained under the control of the GlobalSign CA, the CA ensures that any agreement with the resource owner or services provider is compliant with the requirements for disaster recovery.

6.4.2 CA public key revocation

If a GlobalSign CA public key is revoked the GlobalSign CA will immediately:

- Notify all CAs with which it is cross-certified.

6.4.3 CA private key is compromised

If the private key of the GlobalSign CA is compromised, the corresponding certificate will immediately be revoked. Additional measures will be taken including the revocation of all end user certificates.

6.5 Activation Data

The GlobalSign CA securely stores and archives activation data associated with its own private key and operations.

6.6 Computer Security Controls

The GlobalSign CA implements computer security controls.

6.7 Life Cycle Security Controls

The GlobalSign CA performs periodic development controls and security management controls.

6.8 Network Security Controls

The GlobalSign CA maintains a high-level network of systems security including firewalls. Network intrusions are detected. In specific:

- The GlobalSign CA encrypts connections to the RA, using dedicated administrative certificates.
- The GlobalSign CA website provides certificate based Secure Socket Layer connections and anti-virus protection.
- The GlobalSign CA network is protected by a managed firewall and intrusion detection system.
- Accessing GlobalSign CA databases from outside the CAs network is prohibited.
- Internet sessions for request and delivery of information are encrypted.

6.9 Time-stamping

Not applicable.

7. Certificate and CRL Profiles

This section specifies the certificate format, CRL and OCSP formats.

7.1 Certificate Profile

GlobalSign certificate profiles are available upon request.

7.2 CRL Profile

The GlobalSign CA maintains a record of the CRL profile it uses in an independent technical document. This will be made available at the discretion of the GlobalSign CA, on request from parties explaining their interest.

7.3 OCSP Profile

The GlobalSign CA maintains a record of the OCSP profile it might use in an independent technical document. This will be made available at the discretion of the GlobalSign CA, on request from parties explaining their interest.

8. Compliance Audit And Other Assessment

The GlobalSign CA accepts under condition the auditing of practices and procedures it does not publicly disclose. The GlobalSign CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content the GlobalSign CA accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS and accreditation schemes it publicly claims compliance with.

8.1 Compliance Audit And Other Assessment

Information on GlobalSign's conformance with the requirements of any accreditation scheme can be sought by the organization of such accreditation scheme directly.

GlobalSign has successfully been audited and currently meets the requirements of the accreditation scheme known as WebTrust for CAs. GlobalSign seeks to maintain its accreditation.

GlobalSign accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. GlobalSign accepts this auditing of its own practices and procedures that it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by a party to which GlobalSign owes duty.

The CA evaluates the results of such audits before further implementing them.

8.1.1 Audit process conditions

To carry out the audits there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with GlobalSign nor having any conflicting interests thereof.

An audit is carried out in areas that include but are not limited to the following ones:

- Compliance of GlobalSign operating procedures and principles with the procedures and service levels defined in the CPS.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CPS.
- Adherence to relevant laws.
- Asserting agreed service levels.
- Inspection of audit trails, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

With regard to conformance audits, GlobalSign undertakes the responsibility of the performance of any subcontractors it uses to carry out certification operations including those described in the section below.

8.1.1.1 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, GlobalSign may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. GlobalSign may outsource in part or whole certain aspects of the delivery of its services. Regardless of the partner or agent selected to manage certain parts of the certificate life cycle or operations, GlobalSign remains ultimately in charge of the whole process. GlobalSign will ensure that compliance audits are also applied to such outsourced services. GlobalSign limits its responsibility thereof according to the conditions in this CPS and the GlobalSign CP.

8.1.1.2 Secure Devices and Private Key Protection.

GlobalSign supports the use of secure devices and tamperproof equipment to securely issue, manage and store certificates. GlobalSign uses accredited trustworthy hardware to prevent compromise of its private key.

9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of the GlobalSign CA certificates under this CPS as described in this section.

9.1 Fees

The issuance and management of GlobalSign CA certificates is subject to fees announced on the GlobalSign web site www.globalsign.net or through requested quotes.

9.1.1 Refund policy

GlobalSign accepts requests for refund in writing. Refund requests must be duly justified and addressed to the Legal Services of GlobalSign. GlobalSign reserves its right to endorse or grant and refunds unless they are requested in the framework of a warranty offered by GlobalSign.

9.2 Financial Responsibility

GlobalSign maintains sufficient resources to meet its perceived obligations under this CPS. The GlobalSign CA makes this service available on an “as is” basis. GlobalSign makes available a limited warranty plan published on www.globalsign.net.

9.3 Confidentiality of Business Information

The GlobalSign CA observes personal data privacy rules and confidentiality rules as described in the GlobalSign CPS. Confidential information includes:

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation or suspension of a certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificate and their content.
- Status of a certificate.

GlobalSign does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the GlobalSign CA owes a duty to keep information confidential is the party requesting such information.
- A court order.

The GlobalSign may charge an administrative fee to process such disclosures.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- Only a single certificate is delivered per inquiry by subscriber or relying party.
- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to subscribers nor relying parties. The GlobalSign CA properly manages the disclosure of information to the CA personnel.

The GlobalSign CA authenticates itself to any party requesting the disclosure of information by:

- Presenting an authentication certificate at the request of the subscriber or relying party
- Signing responses to OCSP requests and CRLs.

The GlobalSign CA encrypts all communications of confidential information including:

- The communications link between the CA and the RAs.
- Sessions to deliver certificates and certificate status information.

To incorporate information by reference the GlobalSign CA uses computer-based and text-based pointers that include URLs, etc.

9.4 Privacy of Personal Information

The GlobalSign CA makes available a specific Data Protection Policy for the protection of personal data of the applicant applying for a GlobalSign CA certificate that they make available through their web site. The GlobalSign CA adheres to the documented Privacy Policy of GlobalSign NV available from www.globalsign.net/repository.

The practices and operations of the GlobalSign CA are within the boundaries of the Belgian law of 8 December, 1992, on privacy protection in relation to the processing of personal data as modified by the law of 11 December 1998, implementing the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 p. 0031 – 0050).

The regulation on the protection of personal data in the Belgium implements the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The GlobalSign CA also acknowledges Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The GlobalSign CA operates within the conditions for the protection of personal data asserted in this CPS.

The GlobalSign CA has made appropriate representations before the Belgian Data Protection Commission with regard to the archives of personal data it maintains, collects and processes. The Belgian Data Protection Commission can be contacted by post at: Ministry of Justice, Waterloolaan 115, B-1000 Brussels, Belgium (tel. +32 2 5427206)

9.5 Intellectual Property Rights

The GlobalSign CA owns and reserves all intellectual property rights associated with its databases, web sites, GlobalSign CA digital certificates and any other publication whatsoever originating from GlobalSign CA including this CPS.

The Distinguished names of all CAs of the GlobalSign CA, remain the sole property of GlobalSign, which enforces these rights.

Certificates are and remain property of the GlobalSign CA. The GlobalSign CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of the GlobalSign CA. The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.

The GlobalSign CA owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Representations and Warranties

The GlobalSign CA uses this CPS, associated CPs and a subscriber agreement to convey legal conditions of usage of GlobalSign CA certificates to subscribers and relying parties.

Participants that may make representations and warranties include GlobalSign CA, RAs, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the GlobalSign domain, including the GlobalSign CA, 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.

9.6.1 Subscriber Obligations

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 the 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 the GlobalSign CA CPS and associated policies published in the GlobalSign CA Repository.
- Refraining from tampering with a GlobalSign CA certificate.
- Using GlobalSign CA certificates for legal and authorised purposes in accordance with this CPS.
- Notifying GlobalSign CA or a GlobalSign RA of any changes in the information submitted.
- Ceasing to use a GlobalSign CA certificate if any featured information becomes invalid.
- Ceasing to use a GlobalSign CA certificate when it becomes invalid.
- Removing a GlobalSign CA certificate when invalid from any applications and/or devices they have been installed on.
- Using a GlobalSign CA 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 to GlobalSign CA or any GlobalSign CA directory any material that contains statements that violate any law or the rights of any party.
- Requesting the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a GlobalSign CA certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.

GlobalSign makes available a subscriber agreement in order to ensure that the subscriber is bound under the following terms:

- a) Submit accurate and complete information to GlobalSign in accordance with the requirements of this CPS particularly with regards to registration.
- b) Only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber according to this CPS.
- c) Exercise reasonable care to avoid unauthorized use of its private key.
- d) Under the GlobalSign model the subscriber always generates its own keys, in which case the following terms also apply:
 - Generate subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures;
 - Use a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.
- e) Notify GlobalSign 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).
 - Inaccuracy or changes to the certificate content, as notified to the subscriber.

9.6.2 Relying Party Obligations

A party relying on a GlobalSign CA certificate promises to:

- Have the technical capability to use digital certificates.
- Receive notice of the GlobalSign CA and associated conditions for relying parties.
- Validate a GlobalSign CA certificate by using certificate status information (e.g. a CRL) published by the GlobalSign CA in accordance with the proper certificate path validation procedure.
- Trust a GlobalSign CA certificate only if all information featured on such certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign CA certificate, only as it may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised.

The obligations of the relying party, if it is to reasonably rely on a certificate, are to:

- Verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party.
- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or this CPS.
- Take any other precautions prescribed in the subscriber agreement, GlobalSign certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

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

9.6.2.1 Conveying Relying party obligations

In order to give uninhibited access to revocation information and subsequently invoke Trust in its own services, GlobalSign refrains from implementing an agreement with the relying party with regard to controlling the validity of certificate services with the purpose of binding relying parties to their obligations.

Much like it applies to any other participant of GlobalSign public services, however, the use of GlobalSign resources that relying parties make is implied to be governed by the conditions set out in GlobalSign's policy framework instigated by the GlobalSign CP and the GlobalSign CPS.

Relying parties are hereby notified that the conditions prevailing in this CPS are binding upon them each time they consult a GlobalSign resource for the purpose of establishing trust and validating a certificate.

9.6.3 Subscriber Liability Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CP, subscribers are liable for any misrepresentations they make in certificates to third parties that, reasonably rely on the representations contained therein.

9.6.4 GlobalSign CA Repository and Web site Conditions

Parties (including subscribers and relying parties) accessing the GlobalSign CA Repository and web site agree with the provisions of this CPS and any other conditions of usage that GlobalSign may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. The GlobalSign CA Repositories include or contain:

- Information provided as a result of the search for a digital certificate.
- Information to verify the status of digital signatures created with a private key corresponding to a public key listed in a certificate.
- Information to verify the status of a digital certificate before encrypting data using the public key included in a certificate
- Information published on the GlobalSign CA web site.
- Any other services that GlobalSign CA might advertise or provide through its web site.
- If a repository becomes aware of or suspects the compromise of a private key, it will immediately notify the appropriate RA. The party that operates a Repository has exclusive responsibility of all acts or omissions associated with it.

The GlobalSign CA maintains a certificate repository during the application period and for a maximum of ten years after the expiration or revocation of a certificate. To verify its integrity the complete repository will be made available to the GlobalSign RAs for queries at any time.

Additionally, the GlobalSign CA repository is available to relying parties.

9.6.4.1 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA Repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any

information provided in a certificate. The GlobalSign CA takes steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the GlobalSign Repositories and web site may result in terminating the relationship between the GlobalSign CA and the party.

9.6.4.2 Accuracy of Information

The GlobalSign CA makes every effort to ensure that parties accessing its repositories receive accurate, updated and correct information. The GlobalSign CA, however, cannot accept any liability beyond the limits set in this CPS and the GlobalSign CA insurance policy.

9.6.5 GlobalSign CA Obligations

To the extent specified in the relevant sections of the CP, the GlobalSign CA promises to:

- Comply with this CPS and its amendments as published under <https://www.globalsign.net/repository>
- Provide infrastructure and certification services, including the establishment and operation of the GlobalSign CA Repository and web site for the operation of public certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available.
- Issue electronic certificates in accordance with this CPS and fulfil its obligations presented herein.
- Revoke certificates issued according to this CPS upon receipt of a valid and authenticated request to revoke a certificate from an RA.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Publish CRLs and/or OCSP responses of all suspended and revoked certificates on a regular basis in accordance with this CPS.
- Provide appropriate service levels according to a service agreement.
- Notify relying parties of certificate revocation by publishing CRLs on the GlobalSign CA repository.

The liability of GlobalSign CA under the above stated article for proven damages is limited to 1 Euro for any individual certificate, directly caused by the occurrences listed above. This limit might be reviewed by GlobalSign. GlobalSign might seek additional insurance coverage against risks emanating from the correctness of the information included in a certificate.

To the extent permitted by law the GlobalSign CA cannot be held liable for:

- Any use of certificates, other than specified in this CPS.
- Falsification of transactions.
- Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving certificates.
- Compromise of private keys associated with the certificates.
- Loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates.
- The submission of erroneous or incomplete data from an RA, including identification data, serial numbers and public key values.
- Erroneous or incomplete requests for operations on certificates by the RA.
- Acts of God.

- The use of certificates.
- The use of public or private keys of cross-certified (non-subordinate) CA's and their relying parties.

The GlobalSign CA acknowledges it has no further obligations under this CPS.

9.6.6 Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign network promises to:

- Generate securely an RA administrator key pair, using a trustworthy system directly or through an agent.
- Provide correct and accurate information in their communications with the GlobalSign CA.
- Ensure that the public key submitted to GlobalSign CA is the correct one (if applicable).
- Generating a new, secure key pair to be used in association with a certificate that they request from GlobalSign CA.
- Receive applications for the GlobalSign CA certificates in accordance with this GlobalSign CPS.
- Carry out all verification and authenticity actions prescribed by the GlobalSign CA procedures and this CPS.
- Submit to the GlobalSign CA the applicant's request in a signed message (certificate request).
- Receive, verify and relay to the GlobalSign CA all requests for revocation of a GlobalSign CA certificate in accordance with the GlobalSign CA procedures and the GlobalSign CA CPS.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CPS.

9.6.7 Information incorporated by reference into a digital certificate

The GlobalSign incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the GlobalSign CA CPS.
- Any other applicable certificate policy as may be stated on an issued GlobalSign certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customised elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

9.6.8 Pointers to incorporate by reference

To incorporate information by reference GlobalSign uses computer-based and text-based pointers. GlobalSign may use URLs, OIDs etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

The GlobalSign CA does not warrant:

- 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 the GlobalSign CA warranty policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.7.2 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) is the GlobalSign CA liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

9.8 Limitations of Liability

The total liability of the GlobalSign is limited in accordance with the Limited Warranty Policy of GlobalSign.

Notice is hereby given that a certificate can only be relied upon for transactions involving a monetary value equal or lower than those published on the Limited Warranty Plan. Further information on the warranty conditions can be found at: www.globalsign.net/repository. An overview of the reliance limits is as follows:

Maximum limits in the GlobalSign Limited Warranty Plan for Subscribers

PersonalSign 2 Certificates	2500 EURO
PersonalSign 2 Pro Certificates	2500 EURO
PersonalSign 3 Certificates	37500 EURO
PersonalSign 3 Pro Certificates	37500 EURO
ServerSign Certificates	37500 EURO
ObjectSign Certificates	37500 EURO
HyperSign Certificates	37500 EURO
SureServer Certificates	100000 Dollars
Surserver EDU Certificates	Not applicable

9.9 Indemnities

This section contains the applicable indemnities.

9.9.1 Indemnity

To the extent permitted by law the subscriber agrees to indemnify and hold the GlobalSign CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that the GlobalSign may incur as a result of:

- Failure to protect the subscriber's private key,
- Use a trustworthy system as required

- Taking precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key
- Attend to the integrity of the GlobalSign Root.

9.10 Term and Termination

This CPS remains in force until notice of the opposite is communicated by the GlobalSign CA on its web site or repository.

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

9.11 Individual notices and communications with participants

The 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 as follows. Individuals communications made to the GlobalSign CA must be addressed to legal@globalsign.net or by post to the GlobalSign in the address mentioned in the introduction of this document.

9.12 Amendments

Changes to this CPS are indicated by appropriate numbering.

9.13 Dispute Resolution Procedures

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 of the dispute with a view to seek dispute resolution.

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

9.13.1 Arbitration

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 CPS the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:

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

9.14 Governing Law

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

Each party, including GlobalSign partners, subscribers and relying parties, irrevocably submit to the jurisdiction of the district courts of Leuven, Belgium.

9.15 Compliance with Applicable Law

GlobalSign 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 Survival

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

9.16.2 Severability

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

10. List of definitions

ACCEPT (A CERTIFICATE)

To approve of a digital certificate by a certificate applicant within a transactional framework.

ACCREDITATION

A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.

APPLICATION FOR A CERTIFICATE

A request sent by a certificate applicant to a CA to issue a digital certificate.

ARCHIVE

To store records for period of time for purposes such as security, backup, or audit.

ASSURANCES

A set of statements or conduct aiming at conveying a general intention.

AUDIT

Procedure used to validate compliance with formal criteria or controls.

AUTHENTICATED RECORD

A signed document containing assurances of authentication or a message with a digital signature verified by a valid Class 3 certificate by a relying party.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.

AUTHORISATION

Granting of rights.

AVAILABILITY

The rate of accessibility of information or resources.

HARDWARE MODULE

The complete system of the hardware module used to keep the certificates and securely generate a key pair.

BINDING

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

CERTIFICATE

The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's ones .

CERTIFICATE REVOCATION LIST OR CRL

A list maintained by the CA of certificates that are revoked before their expiration time.

CERTIFICATION AUTHORITY OR CA

An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the GlobalSign CA.

CERTIFICATION PRACTICE STATEMENT OR CPS

A statement of the practices in the management of certificates during all life phases.

CERTIFICATE STATUS SERVICE OR CSS

A service, enabling relying parties and others to verify the status of certificates.

CONTRACT PERIOD

The duration of the GlobalSign CA contract between the Dutch National Register and the CA organization.

CERTIFICATE CHAIN

A hierarchical list certificates containing an end-user subscriber certificate and CA certificates.

CERTIFICATE EXPIRATION

The end of the validity period of a digital certificate.

CERTIFICATE EXTENSION

A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.

CERTIFICATE HIERARCHY

A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.

CERTIFICATE MANAGEMENT

Actions associated with certificate management include, storage, dissemination, publication, revocation, and suspension of certificates.

CERTIFICATE REVOCATION LIST (CRL)

A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to be consulted by relying parties at all times prior to relying on information featured in a certificate.

CERTIFICATE SERIAL NUMBER

A sequential number that uniquely identifies a certificate within the domain of a CA.

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable application form to request a digital certificate.

CERTIFICATION

The process to issue a digital certificate.

CERTIFICATION AUTHORITY (CA)

An authority, such as the GlobalSign CA that issues, suspends, or revokes a digital certificate.

CERTIFICATE POLICY (CP)

A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a certificate. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

CERTIFICATE ISSUANCE

Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with RFC 3647 and RFC 3039

CERTIFICATE SUSPENSION

Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

CERTIFICATE REVOCATION

Online service used to permanently disable a digital certificate before its expiration date

CERTIFICATE REVOCATION LISTS

Online publication of complete and incremental digital certificates revocation lists compliant with RFC 2459

COMMERCIAL REASONABLENESS

A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

COMPROMISE

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

CONFIDENTIALITY

The condition to disclose data to selected and authorised parties only.

CONFIRM A CERTIFICATE CHAIN

To validate a certificate chain in order to validate an end-user subscriber certificate.

DIGITAL CERTIFICATE

A formatted piece of data that relates an identified subject with a public key the subject uses.

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.

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE

Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

END-USER SUBSCRIBER

A subscriber other than another CA.

ENHANCED NAMING

The usage of an extended organisation field (OU=) in an X.509 v.3.0 certificate.

EXTENSIONS

Extension fields in X.509 v.3.0 certificates.

GENERATE A KEY PAIR

A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HASH

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.

IDENTIFICATION

The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

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.

KEY GENERATION PROCESS

The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

KEY PAIR

A private key and its corresponding public key in asymmetric encryption.

NOTICE

The result of notification to parties involved in receiving CA services in accordance with this CPS.

NOTIFY

To communicate specific information to another person as required by this CPS and applicable law.

NOTARISED TIME STAMPING

Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis with up-to-date technology.

OBJECT IDENTIFIER

A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

PKI HIERARCHY

A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.

PRIVATE KEY

A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.

PUBLIC KEY

A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

PUBLIC KEY CRYPTOGRAPHY

Cryptography that uses a key pair of mathematically related cryptographic keys.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

REGISTRATION AUTHORITY OR RA:

An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

RELATIVE DISTINGUISHED NAME (RDN)

A set of attributes that distinguishes the entity from others of the same type.

RELIANCE

To accept a digital signature and act in a way that shows trust in it.

RELYING PARTY

Any entity that relies on a certificate for carrying out any action.

REPOSITORY

A database and/or directory listing digital certificates and other relevant information accessible on-line.

REVOKE A CERTIFICATE

To permanently end the operational period of a certificate from a specified time forward.

SECRET SHARE

A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.

SECRET SHARE HOLDER

An person that holds a secret share.

SHORT MESSAGE SERVICE (SMS)

A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.

SIGNATURE

A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

SIGNER

A person who creates a digital signature for a message, or a signature for a document.

SMART CARD

A hardware token that contains a chip to implement among others cryptographic functions.

STATUS VERIFICATION

Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs

SUBJECT OF A DIGITAL CERTIFICATE

The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.

SUBSCRIBER

The subject of a digital certificate, or a party designated by the subject to apply for the certificate.

SUBSCRIBER AGREEMENT

The agreement between a subscriber and a CA for the provision of public certification services.

SUSPENDED CERTIFICATE

Temporarily discarded certificate, which nevertheless is kept on hold for one week until revocation or reactivation notice is given to GlobalSign CA by the RA.

TRUSTED POSITION

A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

GLOBALSIGN CA REGISTRATION AUTHORITY:

An entity that verifies and provides all subscriber data to the GlobalSign CA.

GLOBALSIGN CA PUBLIC CERTIFICATION SERVICES

A digital certification system made available by GlobalSign CA as well as the entities that belong to the GlobalSign CA domain as described in this CPS.

GLOBALSIGN CA PROCEDURES

A document describing the GlobalSign CA's internal procedures with regard to registration of end users, security etc.

WEB -- WORLD WIDE WEB (WWW)

A graphics based medium for the document publication and retrieval of information on the Internet.

WRITING

Information accessible and usable for reference.

X.509

The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

11. List of acronyms

CA: Certification Authority
RA: Registration Authority
LRA: Local Registration Authority
CEN/ISSS: European Standardisation Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
GSCA: GlobalSign Certification Authority
IETF: Internet Engineering Task Force
ISO: International Standards Organisation
ITU: International Telecommunications Union
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax