GLOBALSIGN™ CPS

CERTIFICATION PRACTICE STATEMENT

IN SUPPORT OF GLOBALSIGN'S PUBLIC CERTIFICATION SERVICES

VERSION 3.0

DATE OF PUBLICATION: JANUARY 99

Ref. 001

GLOBALSIGN CERTIFICATION PRACTICE STATEMENT

GLOBALSIGN, NV/SA

AVENUE DES ARTS - KUNSTLAAN 1-2, B 4

B-1210 BRUSSELS

BELGIUM.

EMAIL: LEGAL@GLOBALSIGN.NET

Quick Summary Of Important CPS Rights And Obligations

PLEASE SEE THE TEXT OF THIS CPS FOR DETAILS. THIS SUMMARY IS INCOMPLETE. MANY OTHER IMPORTANT ISSUES ARE DISCUSSED IN THE CPS.

i. This Certification Practice Statement (*see* definitions) controls the provision and use of GlobalSign's public certification services (*see* definitions) – including certificate (*see* definitions) application [§ 4], application validation [§ 5], certificate issuance [§ 6], acceptance [§ 7], use [§ 8], and suspension and revocation [§ 9].

ii. You (the user) acknowledge that GlobalSign has provided you with sufficient information to become familiar with digital signatures (*see* definitions) and certificates (*see* definitions) before applying for, using, and relying upon a certificate [§ 1.6].

iii. GlobalSign offers different classes of certificates [§ 2.2]. You must decide which class(es) of certificate is right for your needs.

iv. Before submitting a certificate application [§ 4.2], you must generate a key pair [§§ 2.3.3, 4.1] and keep the private key secure [§ 4.1] from compromise (*see* definitions) in a trustworthy (*see* definitions) manner [§ 4.1.1]. Your software system should provide this functionality.

v. You must accept (*see* definitions) a certificate [§ 7.1] before communicating it to others, or otherwise inducing their use of it. By accepting a certificate (*see* definitions), you make certain important representations [§ 7.2].

vi. If you are the recipient of a digital signature or certificate, you are responsible for deciding whether to rely on it. Before doing so, GlobalSign recommends that you check the GlobalSign repository (*see* definitions) to confirm (*see* definitions) that the certificate (*see* definitions) is valid (*see* definitions) and not revoked (*see* definitions), or suspended (*see* definitions) and then use the certificate to verify [§ 8.1] that the digital signature (*see* definitions) was created during the operational period of the certificate by the private key (*see* definitions) corresponding to the public key (*see* definitions) listed in the certificate (*see* definitions), and that the message (*see* definitions) associated with the digital signature (*see* definitions) has not been altered.

vii. You agree to notify [§ 12.10] GlobalSign that is the applicable certification authority (*see* definitions) upon compromise (*see* definitions) of your private key (*see* definitions).

viii. This Certification Practice Statement (*see* definitions) provides various warranties and promises made by GlobalSign [§ 11]. Otherwise, warranties are disclaimed and liability is limited by GlobalSign [§§ 11.2].

ix. The Certification Practice Statement (*see* definitions) contains various miscellaneous provisions [§ 12], requires compliance with applicable export regulations [§ 12.2], indemnifies subscribers [§ 11.5], and prohibits infringement [§ 12.14].

For more information, see GlobalSign's website at **https://www.globalsign.net** or contact customer service at **legal@globalsign.net**.

Acknowledgements

We thank Professor Dumortier and his team at ICRI for the collaboration and assistance that were very important in the development of the GlobalSign CPS.

Furthermore suggestions and editorial comments of the following people in the development of the GlobalSign CPS and adaptation to Belgian Laws and codes of practice are gratefully acknowledged:

Law

Professor Dumortier	Interdisciplinair Centrum voor Recht en Informatica (ICRI) KUL
Samoera Jacobs	GlobalSign NV/SA

Engineering & Technology

Christian Buysschaert	GlobalSign NV/SA
Maarten Willems	GlobalSign NV/SA

Management & Consulting

Audit and Business Controls

Otto Vermeulen	PriceWaterhouseCoopers

Additionally, the Information Security Committee, Electronic Commerce and Information Technology Division, Section Science and Technology of the American Bar Association and its Digital Signature Guidelines initiative in the development of certain widely recognised practices are gratefully acknowledged.

Finally, the MasterCard/Visa specification of the Secure Electronic Transaction (SET) protocol is acknowledged as a source of design principles (such as hierarchy) and a protocol which this CPS seeks to accommodate.

Comments and Suggestions

Editorial comments and suggestions for future revisions of this CPS are solicited from the user community. Please send your comments to: **legal@globalsign.net** or, to GlobalSign, NV/SA, Kunstlaan-Avenue des Arts 1-2, B4, Bruxelles 1210 Brussel, BELGIUM Attn: Legal department. Tel: +32 2 209 05 90, Fax: +32 2 209 05 99.

TABLE OF CONTENTS

1. PREFATORY MATERIAL

THIS SECTION INTRODUCES THE GLOBALSIGN CERTIFICATION PRACTICE STATEMENT (CPS) AND DESCRIBES ITS STRUCTURE AND UNDERLYING CONVENTIONS. IT CONCLUDES WITH A LIST OF ACRONYMS AND ABBREVIATIONS USED IN THE CPS.

1.1 Executive Summary

This GlobalSign Certification Practice Statement presents the practices that GlobalSign in the provision of GlobalSign's public certification services (PCS) employs in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI). It details and controls the certification process, from establishing an CA, commencing CA and repository operations, to enrolling subscribers. The PCS provide for issuing, managing, using, suspending, revoking, and renewing of certificates. The CPS is intended to legally bind and provide notice to all parties that create, use, and validate certificates within the context of the PCS. As such, the CPS plays a central role in governing the PCS, as represented in Figure 1.

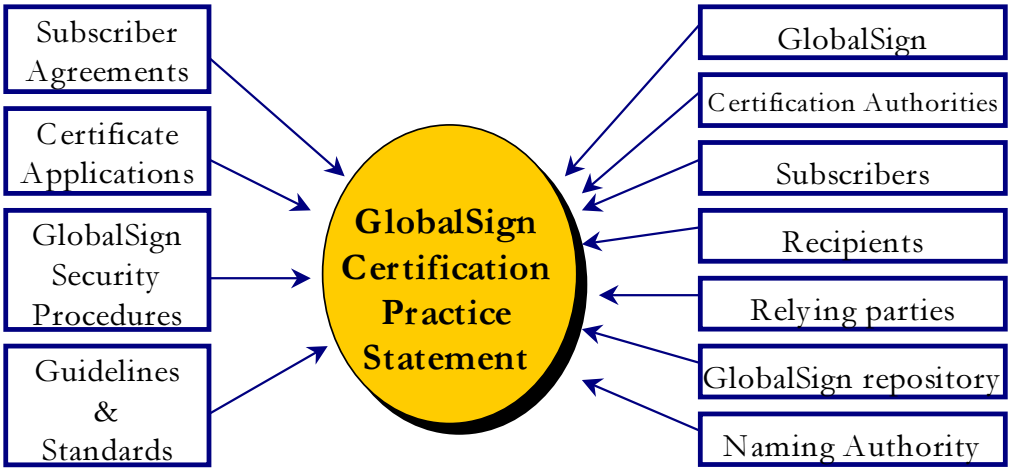

Figure 1 - The central role of the CPS

This CPS governs only a portion of the complement of services offered by GlobalSign. The PCS will inevitably evolve to accommodate other structures in response to market demand.

1.2 Structure of the CPS

The CPS takes a life cycle, or "cradle-to-grave," approach to describing certification processes. It begins with CA establishment and start-up procedures and then covers general CA operations; enrolment; use of certificates; certificate suspension, revocation, and expiration. The benefits of this approach include a chronological presentation of events and compatibility with the anticipated structure of leading private- and public-sector practice statements.

Figure 2 - CPS Life cycle structure

1.3 Citing the CPS

This Certification Practice Statement should be cited in other documents as the "GlobalSign CPS" or the "GlobalSign Certification Practice Statement." It is internally cited as the "CPS," or as "CPS § _" and its appendices as "Appendix § 13._" The CPS is updated periodically. Versions of the CPS are denoted by a version number following "CPS" (*e.g.*, "version 1.0" or "CPS 1.0").

1.4 Definitions

The terms used in the CPS are explained in the appendixes (*see* Appendix 13.1 - Definitions).

1.5 Publication

This CPS is published:

(i) in electronic form within the GlobalSign repository at http://www.globalsign.net/repository

(ii) in electronic form via E-mail from legal@globalsign.net

- Most of the referenced GlobalSign World Wide Web URLs is intended to invoke the HTTP with the Secure Sockets Layer (SSL) security protocol to facilitate "secure mode" record retrieval (when using a browser supporting SSL). Each such record is also available in "unsecure mode" by replacing *https://* with *http://*. The secure mode must be used to access the official version of all Web-accessed documents contained within the GlobalSign repository.
- To assure readers of this CPS of its integrity, it is "hashed" by GlobalSign using a hash function. The hash value is listed in the GlobalSign repository as well as with downloadable versions of the CPS.
- Certain URLs cited in this CPS point to directories rather than to actual messages. This facilitates maintaining such messages in multiple formats for the convenience of the reader. Much of the information referenced by GlobalSign URLs in the CPS is also available as records in electronic and paper form by E-mail request to **legal@globalsign.net**.

1.6 Customer Assistance, Education, and Training

This CPS assumes that the reader is generally familiar with digital signatures, PKIs, and GlobalSign's PCS. If not, we advise some training in the use of public key techniques before the reader applies for a certificate. Educational and training information is accessible from GlobalSign at **http://www.globalsign.net/support.** Additional assistance is available from GlobalSign at **legal@globalsign.net**

ALL PCS APPLICANTS AND SUBSCRIBERS ACKNOWLEDGE THAT (I) THEY HAVE BEEN ADVISED TO RECEIVE PROPER TRAINING IN THE USE OF PUBLIC KEY TECHNIQUES PRIOR TO APPLYING FOR A CERTIFICATE AND THAT (II) DOCUMENTATION, TRAINING, AND EDUCATION ABOUT DIGITAL SIGNATURES, CERTIFICATES, PKI, AND THE PCS ARE AVAILABLE FROM GLOBALSIGN.

1.7 Table of Acronyms and Abbreviations

CA	certification authority
CK	common key
CPS	GlobalSign Certification Practice Statement
CRL	certificate revocation list
CSR	certificate signing request
DAM	draft amendment (to an ISO standard)
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
LRA	local registration authority
NSI	Non-verified subscriber information
PCS	GlobalSign's public certification services
PIN	personal identification number
PKCS	Public Key Cryptography Standards
PKI	public key infrastructure
RDN	Relative Distinguished Name
RSA	a cryptographic system (*see* definitions)
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	uniform resource locator
WWW or Web	World Wide Web
X.509	the ITU-T standard for certificates and their corresponding authentication framework

Table 1 –Table of Acronyms and Abbreviations

2. GLOBALSIGN CERTIFICATION INFRASTRUCTURE

THIS SECTION EXPLAINS THE ARCHITECTURE UNDERLYING THE DISTRIBUTION OF GLOBALSIGN'S PUBLIC CERTIFICATION SERVICES, AS WELL AS CERTIFICATE CLASSES, CERTIFICATE EXTENSIONS, TIME STAMPING, AND THE GLOBALSIGN REPOSITORY.

2.1 Trust Infrastructure

GlobalSign's public certification services (PCS) are designed to support secure electronic commerce and other general security services to satisfy users' technical, business, and personal needs for digital signatures and other network security services. To accomplish this, GlobalSign serves as a trusted third party, issuing, managing, suspending, and revoking certificates in accordance with published practices.

The management and administrative functions of GlobalSign's PCS are established to accommodate a large, public, widely distributed community of users with diverse needs for communications and information security. As a result of such practices, GlobalSign's PCS accommodate a large and geographically dispersed community, enhancing users' trust in these services.

2.1.1 General Discussion of Certificate Issuance and Management

GlobalSign acts as a trusted third party to facilitate the confirmation of the relationship between a public key and a named entity (*see* definition for "naming"). Such confirmation is expressly represented by a certificate – a message which is digitally signed and issued by GlobalSign (*see* CPS § 2.5). The high-level management of this certification process includes registration, naming, appropriate applicant authentication, issuance, revocation, suspension, and audit-trail generation. Naming may be performed principally by GlobalSign or by another party. Naming of subscribers includes a registration process distinct from that used for certificate management which determines when certificates are valid and operational.

GlobalSign currently offers distinct levels of public certification services. Each level, or class, of certificate provides specific functionality and security features. Certificate applicants choose from this set of service qualities according to their needs; they must specify which class of certificate they desire. Depending on the class of certificate desired, certificate applicants may apply electronically to GlobalSign, and they may be required to apply in person by visiting a local registration authority (LRA) or with the necessary assistance of an LRA's delegate. Each certificate issued by GlobalSign corresponds to a specific PCS trust level.

Certificate management also includes the deactivation of certificates and the decommission of the corresponding private keys, through a process involving the revocation and suspension of certificates. Additional CA services may include the listing, distribution, publication, storage, and retrieval of certificates in accordance with their particular intended use.

2.1.2 Security Services

GlobalSign's public certification services support a variety of security mechanisms to protect communications and information assets. Certificates alone do not, however, constitute such a mechanism. Rather, GlobalSign's PCS provide a framework within which security services may be used by other communicating parties. This framework uses digital signatures and their verification to facilitate the protection of communication and computer-based trade and commerce over open data networks and provides a means for determining whether security services are in fact providing the intended assurances.

Certificate-based security services may be used to counter threats to security in a user-defined environment. Users select security mechanisms, security technology, security service agreements, and PCS suitable for the users' anticipated levels of risk, to protect users' communications environments from compromise.

2.2 Certificate Classes

GlobalSign currently supports distinct certificate classes within the CPS. Each class provides for a designated level of trust. The following subsections describe each certificate class. Also, further detail is provided in Table 2 (Certificate Attributes Affecting Trust).

THE DESCRIPTIONS FOR EACH CERTIFICATE CLASS (INCLUDING WITHIN TABLE 2, BELOW) REFLECT APPLICATIONS AND COMMUNICATIONS SYSTEMS THAT HAVE BEEN OR ARE IN THE PROCESS OF BEING IMPLEMENTED BY USERS. THEY DO NOT REPRESENT AN ENDORSEMENT OR RECOMMENDATION BY GLOBALSIGN FOR ANY PARTICULAR APPLICATION OR PURPOSE, AND THEY MUST NOT BE RELIED UPON AS SUCH. USERS MUST INDEPENDENTLY ASSESS AND DETERMINE THE APPROPRIATENESS OF EACH CLASS OF CERTIFICATE FOR ANY PARTICULAR PURPOSE.

2.2.1 Personal Class 1 Certificates

Description: Class 1 certificates are issued to individuals only. Class 1 certificates confirm that a user's e-mail address forms an unambiguous subject name within the GlobalSign repository. Class 1 certificates are communicated electronically to subscribers and added to his or her set of available certificates. They are typically used primarily 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).

Assurance level: Class 1 certificates do not facilitate the authentication of the identity of the subscriber. Rather, 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 Class 1 certificate is considered non-verified subscriber information (NSI). THESE CERTIFICATES PROVIDE THE LOWEST LEVEL OF ASSURANCE OF ALL GLOBALSIGN CERTIFICATES. THEY ARE NOT INTENDED FOR COMMERCIAL USE WHERE PROOF OF IDENTITY IS REQUIRED AND SHOULD NOT BE RELIED UPON FOR SUCH USES. THEY ARE ONLY INTENDED FOR DEMONSTRATION PURPOSES. GLOBALSIGN HAS THE RIGHT, BUT NOT THE OBLIGATION, TO REVOKE CLASS 1 CERTIFICATES UPON COMPROMISE OR FOR OTHER DUE CAUSE. CURRENTLY, REVOCATION OF CLASS 1 CERTIFICATES UPON SUBSCRIBER REQUEST IS PROVIDED ONLY IN THE SOLE DISCRETION OF GLOBALSIGN.

2.2.2 Personal Class 2 Certificates

Description: Class 2 certificates are currently issued to individuals. Class 2 certificates confirm that the application information provided by the subscriber does not conflict with information on the copy of the ID card, driver's license or passport. Class 2 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.

Assurance level: Class 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 copy of the ID card, driver's license or passport.

ALTHOUGH GLOBALSIGN'S CLASS 2 ON-LINE IDENTIFICATION PROCESS IS AN ADVANCED METHOD OF AUTHENTICATING A CERTIFICATE APPLICANT'S IDENTITY, IT DOES NOT REQUIRE THE APPLICANT'S PERSONAL APPEARANCE BEFORE A TRUSTED PARTY (SUCH AS A LOCAL REGISTRATION AUTHORITY. CONSEQUENTLY, THE DECISION TO OBTAIN, USE, OR RELY UPON A CLASS 2 CERTIFICATE SHOULD TAKE INTO ACCOUNT ITS RELATIVE BENEFITS AND LIMITATIONS, AND THE CERTIFICATE SHOULD BE USED ACCORDINGLY.

2.2.3 Personal Class 3 Certificates

Description: Class 3 certificates are issued to individuals. Class 3 certificates provide important assurances of the identity of individual subscribers by requiring their personal (physical) appearance before a Class 3 LRA or its delegate.

Assurance level: Individual Class 3 certificate processes utilise various procedures to obtain probative evidence of the identity of individual subscribers. These validation procedures provide stronger assurances

of an applicant's identity than Class 2 certificates. The practical uses and reliability of Class 3 certificates are bolstered by utilising LRA's (an existing, important, and legally-recognised authentication process).

2.2.4 Secure Server Certificates

Description: – Secure server certificates can provide assurances of the existence and name of various public- and private-sector organisations (such as government agencies and corporations). Validation of secure server certificate applications for organisations includes review by GlobalSign of authorisation records provided by the applicant, third-party business databases, domain name services and independent call-backs ("out-of-band" communications) to the organisation. Secure certificates are used by GlobalSign customers primarily for certain electronic commerce applications such as electronic banking, electronic data interchange (EDI), membership-based on-line services.

Assurance level: Secure server certificate processes utilise various procedures to obtain probative evidence of the identity of individual subscribers. These validation procedures provide stronger assurances of an applicant's identity than Class 2 certificates. For secure server certificates, the requirement for "out-of-band" communication with the business organisation and confirmation of business entity information via third parties provide strong assurance of trustworthiness.

2.2.5 Object Publishing Certificates

Description: – Object publishing certificates can provide assurances of the existence and name of various public- and private-sector organisations (such as government agencies and corporations). Validation of object publishing certificate applications for organisations includes review by GlobalSign of authorisation records provided by the applicant, third-party business databases, domain name services and independent call-backs ("out-of-band" communications) to the organisation. Object publishing certificates are used by GlobalSign customers primarily for the signature of objects like software.

Assurance level: Object publishing certificate processes utilise various procedures to obtain probative evidence of the identity of individual subscribers. These validation procedures provide stronger assurances of an applicant's identity than Class 2 certificates. For object publishing certificates, the requirement for "out-of-band" communication with the business organisation and confirmation of business entity information via third parties provide strong assurance of trustworthiness.

2.3 Certificate Class Properties

Table 2 describes certain properties of each certificate class. Each of the table's headings is described below.

	SUMMARY OF CONFIRMATION OF IDENTITY	CA PRIVATE KEY PROTECTION	CERTIFICATE APPLICANT AND SUBSCRIBER PRIVATE KEY PROTECTION	APPLICATIONS IMPLEMENTED OR CONTEMPLATED BY USERS -*SEE CPS § 2.2 DISCLAIMER & § 2.3.5.*
CLASS 1	Automated unambiguous E-mail address search	CA: trust-worthy software or trustworthy hardware	Encryption software (PIN protected) recommended but not required	Web-browsing & certain E-mail usage
CLASS 2	Automated unambiguous name and E-mail address search plus automated enrolment information check plus verification of a signed copy of the ID card, driver's license or passport	CA: trustworthy hardware	Encryption software (PIN protected) required	Individual and intra- and inter-company E-mail, on-line purchases, on-line subscriptions services, password replacement, software validation

CLASS 3	Automated unambiguous name and E-mail address search plus personal presence & ID documents	CA: trustworthy hardware	Encryption software (PIN protected) required; hardware token recommended but not required	E-banking, corp. database access, personal banking, membership-based on-line services, content integrity services, E-commerce server, software validation
SECURE SERVER	business records, records provided by the applicant and independent call-backs	CA: trustworthy hardware	Encryption software (PIN protected) required; hardware device recommended but not required	Secure web-server communication
OBJECT PUBLISHING	business records, records provided by the applicant and independent call-backs	CA: trustworthy hardware	Encryption software (PIN protected) required; hardware token recommended but not required	Secure object signing

Table 2 - Certificate Properties Affecting Trust

Each class of certificate is characterised by a different level of the following properties: confirmation of identity (such as through personal presence or investigation), CA private key protection (and assurance of appropriate use), certificate applicant and subscriber private key protection, and operational controls. While the certificates (and GlobalSign's supporting products and services) possess many other properties, those listed in Table 2 provide a framework for distinguishing some of their aspects that affect their relative trust. Each property is explained below:

2.3.1 Confirmation of Subscriber Identity

This refers to various actions taken by GlobalSign to validate certificate applicants' identity and confirm the information they provide during the application process. The type, scope, and extent of confirmation depends upon the class of certificate, the type of applicant, and other factors. The particular confirmation methods and their rigor depend upon the class of certificate. Confirmation is further described in CPS § 5.

2.3.2 GlobalSign Private Key Protection

GlobalSign's private key is secured against compromise via trustworthy hardware products. However, Class 1 CA (*see* Figure 4) may secure the secrecy of their private keys via encryption software alone. *See* CPS § 4.1 (Key Generation and Protection).

2.3.3 Certificate Subscriber (and Applicant) Private Key Protection

The secrecy of the private keys of certificate subscribers (and applicants) must be protected through the use of encryption software or hardware tokens (such as smart cards or PC cards) as specified in this CPS. *See* CPS § 4.1 (Key Generation and Protection).

GLOBALSIGN NEITHER GENERATES NOR HOLDS THE PRIVATE KEYS OF CERTIFICATE APPLICANTS OR SUBSCRIBERS. ALSO, GLOBALSIGN CANNOT ASCERTAIN OR ENFORCE ANY PARTICULAR PRIVATE KEY PROTECTION REQUIREMENTS OF ANY CERTIFICATE APPLICANT OR SUBSCRIBER.

2.3.4 Possible Applications Supported

The examples listed in Table 2, above, simply reflect GlobalSign's understanding of existing uses of the various certificate classes. As GlobalSign observes new PCS usage patterns, it will consider providing a specific organisational structure that responds to such patterns.

THE USE OF CERTIFICATES DOES NOT CONVEY EVIDENCE OF AUTHORITY ON THE PART OF ANY USER TO ACT ON BEHALF OF ANY PERSON OR TO UNDERTAKE ANY PARTICULAR ACT. VERIFIERS OF DIGITALLY SIGNED MESSAGES ARE SOLELY RESPONSIBLE FOR EXERCISING DUE DILIGENCE AND REASONABLE JUDGMENT BEFORE RELYING ON CERTIFICATES AND DIGITAL SIGNATURES. A CERTIFICATE

DOES NOT GRANT FROM A CA ANY RIGHTS OR PRIVLEDGES EXCEPT AS PROVIDED IN THIS CPS.

2.3.5 Operational Controls

Operational controls refer to the organisational, human resources, and other management-oriented controls implemented for each class of certificate. Such controls include limits on who is permitted to obtain certificates, requirements concerning the training and education of GlobalSign personnel, policies establishing the separation of duties within GlobalSign, documentation requirements, and prescribed procedures and audits. Many of these controls are identified in CPS § 3 (Foundation for Certification Operations).

2.4 Extensions and Enhanced Naming

2.4.1 Extension Mechanisms and the Authentication Framework

The PCS facilitate the use of X.509 v1, v2, and v3 certificates. X.509 v3 certificates expand the capabilities of v1 and v2, including the ability to add certificate extensions. This capability, a standard component of GlobalSign's PCS, augments the standard authentication services model.

2.4.2 Standard and Service-Specific Extensions

The X.509 "Amendment 1 to ISO/IEC 9594-8:1995" defines a number of extensions. These provide various management and administrative controls useful for large-scale and multipurpose authentication. GlobalSign's PCS exploit a number of these controls for the purposes intended by X.509. (Note: X.509-compliant user software is assumed to enforce the validation requirements of this CPS. GlobalSign cannot guarantee that such software will support and enforce these controls.)

In addition, this CPS allows users to define additional "private" extensions for purposes or modes of use specific to their application environment. For more information contact info@globalsign.net.

2.4.3 Identification and Criticality of Specific Extensions

The function of each extension is indicated by a standard OBJECT IDENTIFIER value (*see* definition for **X.509**). Additionally, each extension in a certificate is assigned a "criticality" true/false value. This value is set by GlobalSign, possibly on the basis of information provided by the certificate applicant on the certificate application. This value must conform to certain constraints imposed by the organisation responsible for the extension definition.

The presence of a criticality value of *true* upon a specific extension requires all persons validating the certificate to consider the certificate invalid if they lack knowledge of the purposes and handling requirements for any specific extension with criticality value of *true*. If the criticality value of such extension is *false*, all persons shall process the extension in conformance with the applicable definition when performing validation or else ignore the extension.

2.4.4 Certificate Chains and Types of CAs

GlobalSign's PCS use chains of certificates. There are three generic roles a CA may play: root registration authority, CA for another CA, and CA for subscribers. A CA must be a subscriber of another CA. Where a CA is its own root, its self-signed public key shall conform to X.509 v1 format. It can potentially be trusted (based-upon out-of-band authentication mechanisms) without recourse to additional validation during verification of digital signatures (*see* CPS § 8 – Use of Certificates). When *registered* by a root registration authority, however, the CA's certificate may contain extensions.

2.4.5 End-User Subscriber Certificate Extensions

CAs serving end-user subscribers may issue certificates containing extensions defined both by the X.509 Amendment 1 to ISO/IEC 9594-8:1995 and by sponsoring organisations such as Microsoft and Netscape (*see* CPS § 2.4.2).

Briefly, the use of these extensions control the process of issuing and validating certificates. Table 3 describes which extensions are present in particular certificates.

2.4.6 ISO-Defined Basic Constraints Extension

The basic constraint extension serves to delimit the role and position a CA or end-user subscriber certificate plays in a chain of certificates. For example, certificates issued to CAs and subordinate CAs contain a basic constraint extension that identifies them as CA certificates. End-user subscriber certificates contain an extension that constrains the certificate from being a CA certificate.

2.4.7 ISO-Defined Key Usage Extension

The key usage extension serves to limit the technical purposes for which a public key listed in a valid certificate may be used within the GlobalSign PCS. CA certificates may contain a key usage extension that restricts the key to signing certificates, certificate revocation lists, and other data.

2.4.8 ISO-Defined Certificate Policy Extension

The certificate policy extension limits a certificate to the practices required by (or indicated to) relying parties. The certificate policy extension, as implemented in the PCS, points its users to this CPS and qualifies appropriate usage (*see* CPS § 2.4.9.1).

2.4.9 Enhanced Naming and GlobalSign Extensions

All end-user subscriber certificates, except for certain S/MIME v1 certificates, contain an additional "Organisational Unit" field — an X.520 attribute — that contains a brief statement regarding liability and incorporates by reference the complete CPS, such as "**This certificate incorporates by reference, and its use is strictly subject to, the GlobalSign Certification Practice Statement (CPS), available at** http://www.globalsign.net/repository " This or comparable information may be present in application-defined X.509 v3 extensions for display to users by "local" (non-GlobalSign vendor controlled) means. Note: the content of this Organisational Unit field is abbreviated because of the X.509 limitation of 64 bytes. This usage of an Organisational Unit field will be retired when functional and consistent use of X.509 v3 extensions become ubiquitous.

When digital signature-verifying software or hardware (collectively, "verifying software") facilitates the acceptance and use of v3 certificate extensions, the verifying software will display both a reference to the CPS and a set of extensions that describe important portions of it. If the verifying software supports only limited or privately defined v3 extensions, the verifying software may then make use of those application-specific extensions, as appropriate, to equivalently disclose certain critical practice statement sections.

Figure 3 illustrates how GlobalSign has implemented this approach within v3 certificates. Key elements in the figure are explained below.

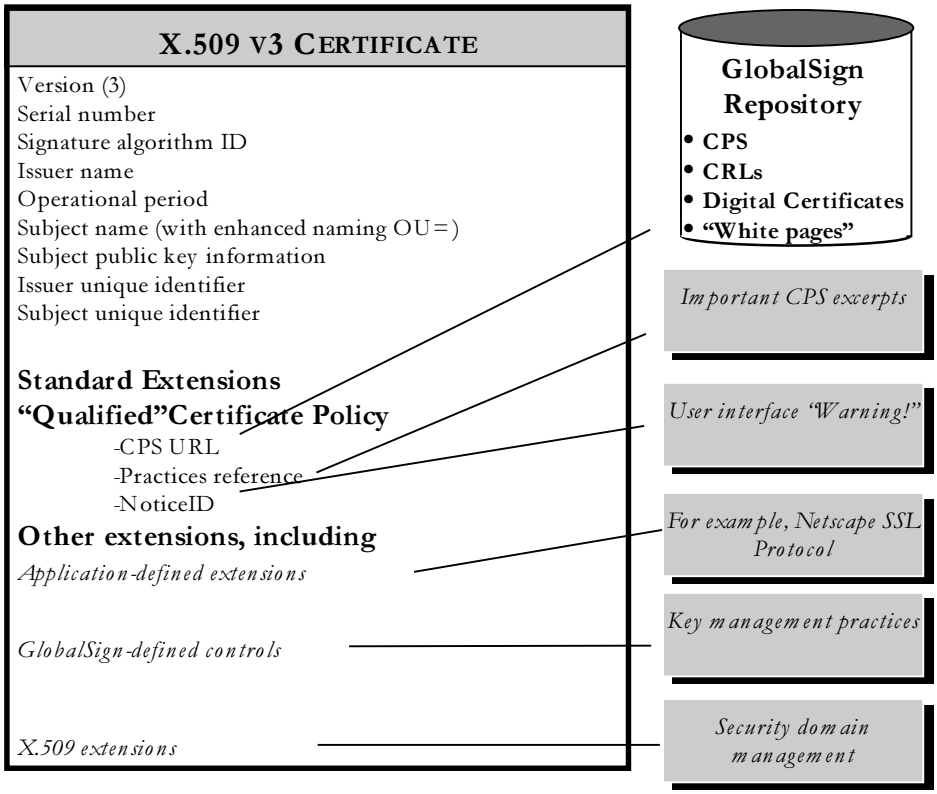

Figure 3 - Certificates and information incorporated by reference

2.4.9.1 Incorporation by Reference

Extensions and enhanced naming are either fully expressed within a certificate or they are at least partially expressed in a certificate with the balance expressed in an external document incorporated by reference in the certificate (*see* definition of **INCORPORATE BY REFERENCE**).

The information contained in the enhanced Organisational Unit field is also present in the **certificatePolicy** extension, when present in a certificate. This CPS constitutes a "certificate policy" as defined by X.509 Amendment 1 to ISO/IEC 9594-8:1995. GlobalSign, acting as a policy-defining authority, has assigned to the CPS an object identifier value which is present in the **certificatePolicy** extension. The definition of this "certificate policy" requires the use of a policy qualifier which GlobalSign has defined to include pointer values, warnings, liability limitations, and warranty disclaimers as described in Table 3 and as follows.

2.4.9.2 Pointers to CPS

Both computer-based pointers (using URLs or other identifiers and mechanisms) and English (human-readable) text or pointers are used, so that certificate users can easily locate and access the CPS and other relevant information.

2.4.9.3 Warnings, Liability Limitations, and Warranty Disclaimers

Each certificate includes a brief statement detailing applicable limitations of liability and disclaimers of warranty. Alternatively, such information may be displayed by a certificate-viewing function, possibly following a hypertext link to a message accessible by users or agents, rather than being embedded in the certificate.

The methods of communicating information (to be displayed by a user) are as follows: an enhanced naming organisational unit attribute; a GlobalSign standard qualifier to a GlobalSign–registered certificate policy (using a standard v3 extension); and other vendors' registered extensions (such as a Netscape–registered "Comment" extension).

Table 3 describes the contents of certificate extensions and the elements of the qualifier to the GlobalSign CPS certificate policy extension.

NAME/CERT.	PURPOSE &	ACCOMPANYING ENGLISH (OR OTHER

EXTENSION FIELDS	DESCRIPTION	HUMAN-READABLE) TEXT
General Extensions for CA : **----------** **basicConstraints** **keyUsage** **General Extensions for End-User Subscriber** **----------** **basicConstraints** **certificatePolicy**	 *See* CPS § 2.4.6 *See* CPS § 2.4.7 *See* CPS § 2.4.6 *See* CPS § 2.4.8	 Non Critical cA = TRUE Non-Critical keyCertSign (Bit 5 set) cRLSign (Bit 6 set) Non Critical cA = FALSE Non Critical *See* CPS § 2.4.9.3
GlobalSign standard qualifier – cpsURLs	A single uniform resource locator indicating the source of this CPS.	**"This certificate incorporates by reference, and its use is strictly subject to, the GlobalSign Certification Practice Statement (CPS), available at** https://www.globalsign.net/repository or similar URL"
GlobalSign standard qualifier-crlURLs	A single uniform resource locator indicating the source of the CRL.	**"The certification revocation list is available at https://www.globalsign.net/company** or similar URL"
GlobalSign standard qualifier – NoticeID	An object identifier referring to a string whose content indicates information about warnings, cautions, warranty disclaimers, and limitations of liability regarding the use of GlobalSign PCS certificates. It is intended to be displayed with every certificate within the user agent (*e.g.*, computer or terminal) certificate viewing function (but it is not embedded in any certificate).	**"WARNING: GLOBALSIGN DISCLAIMS CERTAIN IMPLIED AND EXPRESS WARRANTIES. SEE THE CPS FOR DETAILS. LIMITATION OF LIABILITY TO 100.000 BEF FOR THE IDENTITY IN A CLASS 2, LIMITATION OF LIABILITY TO 1.500.000 BEF FOR THE IDENTITY IN A CLASS 3."** Or similar URL.
GlobalSign standard qualifier – NSINotice	An object identifier referring to a string whose content indicates that the certificate contains data for which GlobalSign provides no assurances of accuracy.	"**Contents of the GlobalSign nonverifiedSubjectAttribute extension value shall not be considered as information confirmed by GlobalSign.**"

Table 3 – GlobalSign Certificate Extensions

2.5 PKI Hierarchy

GlobalSign's public certification services are set up to be implemented within a PKI-entity hierarchy composed of other CAs (including subordinate CAs) .

Within the PKI-entity hierarchy, CAs are interrelated via the relationship of "location subordinate to," which indicates that one CA serves on behalf of another. A CA shall issue CA certificates using either general or enhanced authentication procedures (for CA validation), depending upon the certificate class of the end-user subscriber certificates issued by the last CA in the hierarchy.

In addition, CAs may delegate certain registration functions to one or more RA's and LRAs. Figure 4 provides an overview of the PKI-entity hierarchy. (LRAs are not included in Figure 4, to further simplify the figure).

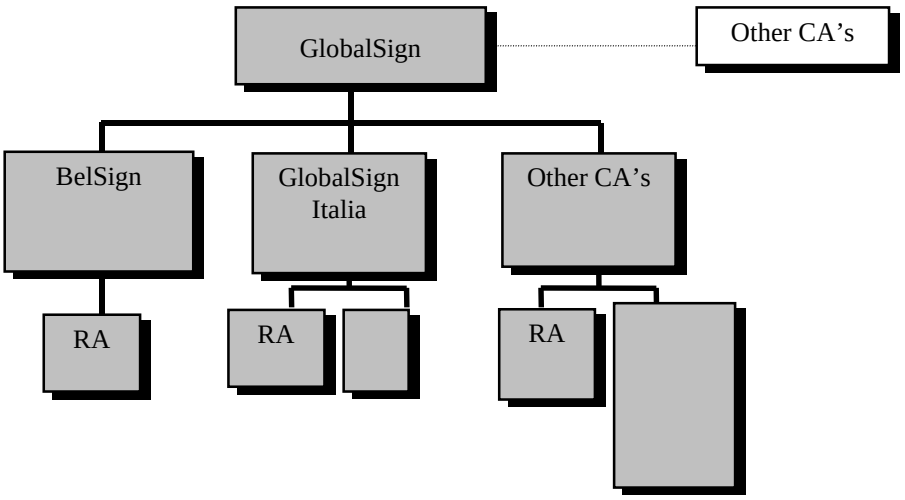

Figure 4 - Simplified PKI hierarchy

2.5.1 Certification Authorities (CAs)

GlobalSign operates in accordance with this CPS and issues, manages, and revokes Class 1-2-3 certificates, secure server and object publishing certificates, as permitted by this CPS.

GlobalSign initial key size is 2048 bits. A trustworthy hardware device is used to create, protect, and destroy the private keys of Class 2, Class 3, secure server and object publishing CA's.

2.5.2 Registration Authorities (RAs)

Registration authorities (RAs) evaluate and approve or reject certificate applications on behalf of and under the exclusive authority of the CA that actually issues the certificates. The CA may have more than one RA.

Without otherwise limiting their authority, RAs may rely upon the following for confirming certificate applicant information: (i) notarial acts that reasonably appear to be performed in good order and (ii) well-recognised forms of identification, such as passports and driver's licenses. RA requirements are presented in CPS § 3.17, below.

2.5.3 Local Registration Authorities (LRAs)

Local registration authorities (LRAs) evaluate and approve or reject certificate applications on behalf of the RA. A RA may have more than one LRA.

Without otherwise limiting their authority, LRAs may rely upon the following for confirming certificate applicant information: (i) notarial acts that reasonably appear to be performed in good order and (ii) well-recognised forms of identification, such as passports and driver's licenses. LRA requirements are presented in CPS § 3.18, below.

2.5.4 GlobalSign Certificate Services and Repository

The GlobalSign certificate services and the GlobalSign repository are a publicly available collection of databases for storing and retrieving certificates and other information related to certificates.

The GlobalSign certificate services include but are not limited to the following: certificates, CRLs and other suspension and revocation information.

The GlobalSign repository includes but is not limited to the following: current and prior versions of the GlobalSign CPS, and other information as prescribed by GlobalSign from time to time.

2.5.5 Publication by the GlobalSign Certificate Services and Repository

The GlobalSign certificate services and the GlobalSign repository will act promptly to publish certificates, amendments to the CPS, notices of certificate suspension or revocation, and other information, consistent with this CPS and applicable law.

The GlobalSign certificate services and the GlobalSign repository are accessible at http://secure.globalsign.net and http://www.globalsign.net/repository and by other communications methods as may be designated by GlobalSign from time to time.

GlobalSign may publish both within and outside of the GlobalSign certificate services a subscriber's certificate and CRL-related data. This CPS prohibits accessing of any data in the certificate services (or data otherwise maintained by GlobalSign) that is declared confidential by the CPS and/or by the GlobalSign certificate services, unless authorised by GlobalSign.

3. FOUNDATION FOR CERTIFICATION OPERATIONS

THIS SECTION ESTABLISHES THE FOUNDATION AND CONTROLS FOR TRUSTWORTHY PCS OPERATIONS. IT INCLUDES THE OPERATING REQUIREMENTS FOR GLOBALSIGN'S PCS, INCLUDING RECORD KEEPING, AUDITING, AND PERSONNEL REQUIREMENTS. IT ALSO PRESENTS THE OBLIGATIONS OF GLOBALSIGN UPON THE TERMINATION OR CESSATION OF ITS OPERATIONS.

NOTE: CERTIFICATE APPLICATION PROCEDURES ARE PRESENTED IN CPS §4.

3.1 Conformance to this CPS

GlobalSign shall conform to this CPS in performing their respective services.

3.2 Trustworthiness

GlobalSign shall utilise only trustworthy systems in performing their respective services.

3.3 Financial Responsibility

GlobalSign shall have sufficient financial resources to maintain their operations and perform their duties, and GlobalSign must be reasonably able to bear the risk of liability to subscribers and recipients of certificates and other persons who may rely on the certificates they issue. GlobalSign shall also maintain insurance coverage for errors and omissions.

3.4 Records Documenting Compliance

GlobalSign shall maintain records in a trustworthy fashion, including

(i) documentation of their own compliance with the CPS, and

(ii) documentation of actions and information that is material to each certificate application and to the creation, issuance, use, suspension, revocation, expiration, and renewal or re-enrollment of each certificate it issues. These records shall include all relevant evidence in GlobalSign's possession regarding

- the identity of the subscriber named in each certificate (except for Class 1 certificates, for which only a record of the subscriber's unambiguous E-mail address is maintained),
- the identity of persons requesting certificate suspension or revocation (except for Class 1 certificates),
- other facts represented in the certificate,
- time stamps, and
- certain foreseeable material facts related to issuing certificates.

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete. GlobalSign may require a subscriber or its agent to submit documents to enable GlobalSign to comply with this section.

3.5 Time Stamping

Time stamping is intended to enhance the integrity of GlobalSign's PCS and the trustworthiness of certificates and to contribute to the non-repudiation of digitally signed messages. Time stamping creates a notation that indicates (at least) the correct date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation. All time stamps reflect Greenwich mean time (GMT) and adopt the Universal Time Conventions (UTC).

The following data shall be time stamped, either directly on the data or on a correspondingly trustworthy audit trail, by GlobalSign:

- certificates,
- CRLs and other suspension and revocation database entries,
- each version of the CPS,
- customer service messages, and
- other information, as prescribed by this CPS.

TIME STAMPING IS NOT YET AVAILABLE.

3.6 Records Retention Schedule

GlobalSign shall retain in a trustworthy fashion Class 2 records for at least five (5) years and Class 3, Secure Server and Object Publishing Highest Assurance records for at least thirty (30) years after the date a certificate is revoked or expires. Such records may be retained as either retrievable computer-based messages or paper-based documents.

3.7 Audit

GlobalSign shall implement and maintain trustworthy systems to preserve an audit trail for all material events, such as key generation and certificate application, validation, suspension, and revocation. A certified public accountant with demonstrated expertise in computer security or an accredited computer security professional shall audit the operations of GlobalSign at least annually, to evaluate its compliance with this CPS and other applicable agreements, guidelines, procedures, and standards.

GlobalSign's receipt of such third-party audit reports constitutes neither endorsement nor approval on the part of GlobalSign of the content, findings, and recommendations of such reports. GlobalSign may review such reports to protect GlobalSign's PCS. Since GlobalSign is not the author of such audit reports, and is therefore not responsible for their content, GlobalSign does not express any opinion on such audit reports and shall not be held responsible for any damages to anyone resulting from GlobalSign's reliance on such audit reports.

3.8 Contingency Planning and Disaster Recovery

GlobalSign shall implement, document, and periodically test appropriate contingency planning and disaster recovery capabilities and procedures, consistent with this CPS and the BSP.

3.9 Availability of CA Certificates

GlobalSign shall make copies of their own certificates (*i.e.,* those in which GlobalSign is the subject) and any revocation data (where applicable) available to any person who has and desires to duly verify a digital signature that is verifiable by reference to such a certificate.

3.10 Publication by GlobalSign

GlobalSign must publish their certificate, all issued certificates, revocation data, and this CPS.

3.11 Confidential Information

The following information shall be considered received and generated in confidence by GlobalSign and may not be disclosed except as provided below:

- Subscriber agreements and certificate application records (except for information placed in a certificate or repository per this CPS),
- transactional records (both full records and the audit trail of transactions),
- PCS audit trail records created or retained by GlobalSign,
- PCS audit reports created by GlobalSign, or their respective auditors (whether internal or public),

- contingency planning and disaster recovery plans, and
- security measures controlling the operations of GlobalSign hardware and software and the administration of certificate services and designated enrollment services.

GlobalSign shall not disclose or sell applicant names or other identifying information, and neither shall share such information, except in accordance with this CPS. Note, however, that the GlobalSign repository shall contain certificates, revocation and other information (*see* CPS §§ 2.5.3, 2.5.4 regarding theGlobalSign certificate services and GlobalSign repository).

Each subscriber has the right to consult the information GlobalSign keeps about him. The request shall be done by digitally signed messages consistent with the requirements of this CPS, or in writing via registered mail. GlobalSign shall answer the request within five (5) business days.

Voluntary Release / Disclosure of Confidential Information.

GlobalSign shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release from (i) the person to whom the GlobalSign owes a duty to keep information confidential and (ii) the person requesting confidential information (if not the same person); or a court order. GlobalSign may require that the requesting person pay a reasonable fee before disclosing such information.

3.12 Personnel Management and Practices

GlobalSign shall formulate and follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. Such practices shall be consistent with this CPS.

3.12.1 Trusted Positions

All employees, contractors, and consultants of GlobalSign (collectively, "personnel") that have access to or control over cryptographic operations that may materially affect the GlobalSign issuance, use, suspension, or revocation of certificates, including access to restricted operations of the GlobalSign repository, shall, for purposes of this CPS, be considered as serving in a trusted position. Such personnel include, but are not limited to, all customer service personnel, system administration personnel, designated engineering personnel, and executives who are designated to oversee the GlobalSign trustworthy system infrastructures.

3.12.2 Investigation and Compliance

GlobalSign shall conduct an initial investigation of all personnel who are candidates to serve in trusted positions to make a reasonable attempt to determine their trustworthiness and competence. GlobalSign shall conduct periodic investigations of all personnel who serve in trusted positions to verify their continued trustworthiness and competence in accordance with GlobalSign's personnel practices or equivalent.

3.12.3 Removal of Persons in Trusted Positions

All personnel who fail an initial or periodic investigation shall not serve in a trusted position. The removal of any person serving in a trusted position shall be at the sole discretion of GlobalSign.

3.13 Accreditation

3.13.1 Approval of Software and Hardware Devices

All PCS-related hardware and software shall be approved by GlobalSign, an authorized GlobalSign consultant, or other recognised authority (as designated from time to time by GlobalSign), as appropriate.

3.13.2 Personnel in Trusted Positions

All personnel serving in trusted positions shall be accredited.

3.13.3 Organisational Good Standing

GlobalSign shall be in good standing with (and, where applicable, accredited, certified, or licensed by) applicable agencies and authorities whose rules and regulations materially affect GlobalSign's trustworthiness and as required by law or contract.

3.14 GlobalSign Key Generation

GlobalSign shall securely generate and protect its own private key(s), using a trustworthy system, and take necessary precautions to prevent its loss, disclosure, modification, or unauthorised use.

GlobalSign shall implement and document key generation procedures, consistent with this CPS.

3.15 Secret Sharing

GlobalSign shall use secret sharing (*see* definitions), using authorised secret share holders, to enhance the trustworthiness of their private key(s) and provide for their keys' recovery.

3.15.1 Hardware Protection

GlobalSign must use approved trustworthy hardware cryptomodules for all operations requiring the use of their private key, except for Class 1 CAs, which may use trustworthy software with secret sharing.

3.15.2 Representations by GlobalSign

GlobalSign intending to distribute secret shares of its private key(s), represents and warrants to all applicable entities that it lawfully possesses private key(s) intended to be secret shared and has the authority to transfer them to authorised secret share holders.

3.15.3 Acceptance of Secret Shares by Secret Share Holders

For a secret share holder to accept a secret share, a majority of the designated secret share holders must have personally observed the creation, re-creation, and distribution of the share and its subsequent chain of custody.

Each secret share holder must receive the secret share within a physical medium, such as a GlobalSign-approved hardware token. Once the secret share holder is satisfied that his or her inspection of the delivered secret share is complete, he or she shall acknowledge acceptance of the secret share by signing and returning to GlobalSign a secret share acceptance form provided by GlobalSign.

3.15.4 Safeguarding the Secret Share

The secret share holder shall use trustworthy systems to protect the secret share against compromise. Except as provided in this CPS, the secret share holder agrees that he or she shall not

- divulge, disclose, copy, make available to third parties, or make any unauthorised use whatsoever of the secret share,
- reveal (expressly or implicitly) that he or she, or any other secret share holder, is a secret share holder, or
- store the secret share in a location that fails to provide for its recovery in the event the secret share holder becomes incapacitated or unavailable (except when the secret share is being used for authorised purposes).

3.15.5 Availability and Release of Secret Shares

The secret share holder shall make the secret share available to authorised entities (listed in the secret share holder acceptance form) only when provided with proper authorisation by an authenticated record (see next paragraph). In the event of a disaster situation (when declared by the secret share issuer), the secret share holder shall report to a disaster recovery site in accordance with instructions from the secret share issuer. Prior to travelling to any contingency/disaster recovery site and releasing the secret share, the secret share holder shall authenticate the declaration of the secret share issuer as specified on the secret share acceptance form (except where prohibited by law or legal process, such as concerning certain criminal investigations). This procedure will include the use of a challenge phrase (communicated from the secret

share issuer to the secret share holder) to ensure that the secret share holder is not tricked into travelling to the wrong location thereby incapacitating the secret share issuer's ability to recover. At the disaster recovery site, the secret share holder shall physically deliver (in person) the secret share in order to participate in the disaster recovery procedure.

The secret share holder may rely upon any instruction, document, message, record, instrument, or signature he or she reasonably believes to be genuine, provided he or she authenticates such declaration of the secret share issuer in the manner provided by the preceding paragraph. The secret share issuer will provide the secret share holder with a sample set of all signatures to be used to authenticate the instructions of the secret share issuer.

3.15.6 Record Keeping by Secret Share Issuers and Holders

Secret share issuers and holders shall keep records of activities pertaining to all secret share materials. The secret share holder shall provide information regarding the status of the secret share to the secret share issuer or its designee upon authenticated request.

3.15.7 Secret Share Holder Liability

The secret share holder shall perform his or her obligations under this CPS and must act in a reasonable and prudent manner in all respects. The secret share holder shall notify the secret share issuer of any loss, theft, improper disclosure, or compromise of the secret share immediately upon learning of it. The secret share holder is not responsible for failure to fulfil his or her obligations due to causes beyond his or her reasonable control but shall be liable for improper disclosure of secret shares or failure to notify the secret share issuer of improper disclosure or compromise through his or her fault, including negligence or recklessness.

3.15.8 Indemnity by Secret Share Issuer

The secret share issuer agrees to indemnify and hold harmless the secret share holder from all claims, actions, damages, judgements, arbitration fees, expenses, costs, attorney's fees, and other liabilities incurred by the secret share holder related to the secret share that are not caused or contributed to by the secret share holder's fault, including negligence, or recklessness.

3.16 Security Requirements

3.16.1 Communication Security Requirements

All communications pursuant to this CPS among GlobalSign and the other parties in the PCS must use an application that provides appropriate security mechanisms commensurate with the attendant risks. Without limiting the generality of the foregoing, computer-based notices, corresponding notice acknowledgements, and any other communications affecting the security of the PCS shall also be appropriately secured.

3.16.2 Facilities Security Requirements

GlobalSign shall operate trustworthy facilities that are in substantial conformance with the BSP, or equivalent.

3.17 Registration Authority (RA) Requirements

RAs serve in trusted positions (*see* CPS § 3.12 – Personnel Management and Practices). The minimum requirements for a RA depend upon the class of certificate application that an RA is authorised to approve. Such requirements are presented in Table 4.

3.18 Local Registration Authority (LRA) Requirements

LRAs serve in trusted positions (*see* CPS § 3.12 – Personnel Management and Practices). The minimum requirements for an LRA depend upon the class of certificate application that an LRA is authorised to approve. Such requirements are presented in Table 4.

	CLASS 1	CLASS 2	CLASS 3
EDUCATION	Not applicable.	Not applicable.	At least 2 yrs. of college or equivalent registration and certification experience.
TRAINING	Paper based manual	Paper based manual	1/2 day LRA apprenticeship before commencing RA/LRA employment.
ACCREDITATION	After identification.	After identification.	After training. Document of good conduct, document of respect privacy and document of training.
AUDIT	Annually	Annually	Annually
CONTRACT	Yes.	Yes.	Yes
RECORD KEEPING	Per CPS § 3.4.	Per CPS § 3.4.	Per CPS § 3.4.

	SECURE SERVER	OBJECT PUBLISHING
EDUCATION	At least 2 yrs. of college or equivalent registration and certification experience.	At least 2 yrs. of college or equivalent registration and certification experience.
TRAINING	1/2 day LRA apprenticeship before commencing RA/LRA employment.	1/2 day LRA apprenticeship before commencing RA/LRA employment.
ACCREDITATION	After training. Document of good conduct, document of respect privacy and document of training.	After training. Document of good conduct, document of respect privacy and document of training.
AUDIT	Annually	Annually
CONTRACT	Yes.	Yes.
RECORD KEEPING	Per CPS § 3.4.	Per CPS § 3.4.

Table 4 – RA and LRA Requirements

3.19 Termination or Cessation of CA Operations

The following obligations are intended to reduce the impact of a termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, and certain remedies.

3.19.1 Requirements Prior to Cessation

Before ceasing to act as a CA, GlobalSign must:

(i) Provide to the subscriber of each unrevoked or unexpired certificate it issued ninety (90) days notice of its intention to cease acting as a CA.

(ii) Revoke all certificates that remain unrevoked or unexpired at the end of the ninety (90) day notice period, whether or not the subscribers have requested revocation.

(iii) Give notice of revocation to each affected subscriber, as detailed in CPS § 9.

(iv) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding certificates.

(v) Make reasonable arrangements for preserving its records.

3.19.2 Re-issuance of Certificates by a Successor CA

To provide uninterrupted CA services to its certificate applicants and subscribers, a discontinuing CA must arrange with another such authority, subject to the other CA's prior written approval, for re-issuance of its outstanding subscriber certificates. In reissuing a certificate, the succeeding CA (not to be confused with a subordinate CA) subrogates to the rights and defences of the discontinuing CA and, to the extent agreed in writing between the discontinuing and succeeding CA, assumes all of its obligations and liabilities regarding outstanding certificates. Unless a contract between the discontinuing CA and a subscriber provides otherwise, and subject to the succeeding CA's written approval, the CPS will remain in effect under the succeeding CA as under the original CA.

The requirements of this subsection may be varied by contract, provided such modifications affect only the contracting parties.

4. CERTIFICATE APPLICATION PROCEDURES

THIS SECTION DESCRIBES THE CERTIFICATE APPLICATION PROCESS. IT INCLUDES THE REQUIREMENTS FOR KEY PAIR GENERATION AND PROTECTION AND LISTS THE INFORMATION REQUIRED FOR EACH CLASS OF CERTIFICATE.

All persons (other than GlobalSign) desiring a certificate shall contemporaneously complete the following general procedures for each certificate application:

- generate a key pair and demonstrate to GlobalSign that it is a functioning key pair,
- protect the private key (of this key pair) from compromise,
- submit a certificate application (and subscriber agreement), including the public key of this key pair, to GlobalSign,
- prove their identity

4.1 Key Generation and Protection

The following procedures are applicable to all entities generating keys as provided in this CPS.

4.1.1 Holder Exclusivity; Controlling Access to Private Keys

Unless otherwise permitted by this CPS, each certificate applicant shall securely generate his, her, or its own private key, using a trustworthy system, and take necessary precautions to prevent its compromise, loss, disclosure, modification, or unauthorised use. It is understood that subscribers (and certificate applicants) will generally use non-GlobalSign products that provide appropriate protection to keys.

EACH CERTIFICATE APPLICANT (AND, UPON APPROVAL, EACH SUBSCRIBER) ACKNOWLEDGES THAT SUCH PERSON, AND NOT GLOBALSIGN, IS EXCLUSIVELY RESPONSIBLE FOR PROTECTING HIS, HER, OR ITS PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE.

Users and GlobalSign agree not to monitor, interfere with, or reverse engineer the technical implementation of the PCS except as explicitly permitted by this CPS or upon prior written approval of GlobalSign.

4.1.2 Delegation of Responsibilities for Private Keys

Delegation, if it occurs, does not relieve the delegator of his, her or its responsibilities and liabilities concerning the generation, use, retention, or proper destruction of his, her, or its private key.

4.2 Certificate Application Information and Communication

Certificate application information includes the items listed in the following Table 5. *Not all of the following information will appear in a certificate (see* Figure 3 - Certificates and Information Incorporated by Reference). *Note*: The items of such information not included in the certificate will be kept confidential by GlobalSign (*see* CPS § 3.11).

CLASS OF CERTIFICATE	REQUIRED CERTIFICATE APPLICATION INFORMATION
CLASS 1	**INDIVIDUALS:** *REQUIRED INFORMATION* • Subject public key • E-mail address • Country *OPTIONAL*

	• Other information as prescribed by GlobalSign *METHOD OF COMMUNICATING APPLICATION* GlobalSign communicates an on-line enrolment process to the certificate applicant. By completing this on-line dialog via a secure channel, the certificate applicant then affirms that the certificate applicant information is accurate. Upon completion of specified validation procedures, GlobalSign sends a certificate to the certificate applicant.
CLASS 2	**INDIVIDUALS:** *REQUIRED INFORMATION* • E-mail address • Legal name (in the form of a common name) • Country • Subject public key • Identification data • Challenge phrase (to later authenticate subscriber to GlobalSign) • Payment information *OPTIONAL* • Other information as prescribed by GlobalSign *METHOD OF COMMUNICATING APPLICATION* GlobalSign communicates an on-line enrolment process and a subscriber agreement to the certificate applicant. By completing this on-line dialog via a secure channel, the certificate applicant then affirms that (i) the certificate applicant information is accurate and (ii) he or she has read, understands, and agrees to the term of the subscriber agreement. The certificate applicant proves his identity by submitting a signed copy of at least one (1) form of identification. Upon completion of specified validation procedures, GlobalSign sends E-mail to the E-mail address that was previously provided by the certificate applicant in the certificate application. This E-mail contains an URL (and optionally, a draft of information content to be included in the certificate) that authorises the certificate applicant to obtain a certificate from GlobalSign.

CLASS 3	**INDIVIDUALS:**
	
	REQUIRED INFORMATION **– *SAME AS CLASS 2, PLUS:***
	• Subscriber agreement and registration form acknowledged by a LRA (to fulfil the "personal presence" requirement) upon presentation of at least one (1) form of identification by the certificate applicant.
	• Proof of professional context
	  • for an employee articles of incorporation and confirmation by legal representative
	  • for an independent: extract of register of commerce
	  • for someone with a liberal profession: official document from the professional group and member card
	
	OPTIONAL **– *SAME AS CLASS 2, PLUS:***
	• Other information as prescribed by GlobalSign
	
	METHOD OF COMMUNICATING APPLICATION
	GlobalSign communicates an on-line enrolment process and a subscriber agreement to the certificate applicant. By completing this on-line dialog via a secure channel, the certificate applicant then affirms that (i) the certificate applicant information is accurate and (ii) he or she has read, understands, and agrees to the term of the subscriber agreement. The certificate applicant proves his identity by submitting a signed copy of at least one (1) form of identification and other documents when going personally to the LRA. Upon completion of specified validation procedures, GlobalSign sends E-mail to the E-mail

	address that was previously provided by the certificate applicant in the certificate application. This E-mail contains an URL (and optionally, a draft of information content to be included in the certificate) that authorises the certificate applicant to obtain a certificate from GlobalSign.

SECURE SERVER	**BUSINESS ENTITIES:**
	
	REQUIRED INFORMATION
	• Domain name
	• Legal Name of the Organisation
	• Organisational unit (if applicable)
	• Street, city, postal/zip code, country
	• Technical and billing contact persons and legal representative
	• VAT-number
	• Trade Register number
	• Server Software
	• Payment Information
	• Proof of right to use name (via domain name service)
	• Proof of existence of the Organisation (via third-party database checks and out-of-band verification)
	• The following information shall be submitted by fax and courier to GlobalSign:
	  • Proof of organisational status:
	  – For business: statutes of the company
	  – For universities: official letter from office of dean
	  – For government organisations: official letter from a properly-authorised person
	  • Registration form signed and properly filled in
	  • Server agreement signed
	
	OPTIONAL
	• Other information as prescribed by GlobalSign
	
	METHOD OF COMMUNICATING APPLICATION
	GlobalSign communicates an on-line enrolment process and a server agreement to the certificate applicant. The certificate prints out the online documents and sends them with the proof of existence of the organisation to the (L)RA. The applicant then affirms that (i) the certificate applicant information is accurate and (ii) he or she has read, understands, and agrees to the term of the server agreement. The applicant creates the key pair and sends the public key by E-mail to the CA. Upon completion of specified validation procedures, GlobalSign sends E-mail to the E-mail address that was previously provided by the certificate applicant in the certificate application. This E-mail contains an URL (and optionally, a draft of information content to be included in the certificate) that authorises the certificate applicant to obtain a certificate from GlobalSign.

OBJECT PUBLISHING	**BUSINESS ENTITIES:** *REQUIRED INFORMATION* • Domain name • Legal Name of the Organisation • Organisational unit (if applicable) • Street, city, postal/zip code, country • Technical and billing contact persons and legal representative • VAT-number

	• Trade Register number
	• Payment Information
	• Proof of right to use name (via domain name service)
	• Proof of existence of the Organisation (via third-party database checks and out-of-band verification)
	• The following information shall be submitted by fax and courier to GlobalSign
	  • Proof of organisational status:
	  – For business: statutes of the company
	  – For universities: official letter from office of dean
	  – For government organisations: official letter from a properly-authorised person
	  • Registration form signed and properly filled in
	  • Subscriber agreement signed
	  • Copy of identity card/passport/driver's license from legal representative of the Organisation
	OPTIONAL
	• Other information as prescribed by GlobalSign
	
	METHOD OF COMMUNICATING APPLICATION
	GlobalSign communicates an on-line enrolment process and a subscriber agreement to the certificate applicant. By completing this on-line dialog via a secure channel, the certificate applicant then affirms that (i) the certificate applicant information is accurate and (ii) he or she has read, understands, and agrees to the term of the subscriber agreement. The certificate applicant proves his identity by submitting a signed copy of at least one (1) form of identification and other documents to the (L)RA. Upon completion of specified validation procedures, GlobalSign sends E-mail to the E-mail address that was previously provided by the certificate applicant in the certificate application. This E-mail contains an URL (and optionally, a draft of information content to be included in the certificate) that authorises the certificate applicant to obtain a certificate from GlobalSign.

Table 5 – Required Certificate Application Information

5. VALIDATION OF CERTIFICATE APPLICATIONS

THIS SECTION PRESENTS THE REQUIREMENTS FOR VALIDATION OF CERTIFICATE APPLICATIONS TO BE PERFORMED BY GLOBALSIGN OR BY AN AUTHORISED (LOCAL) REGISTRATION AUTHORITY. IT ALSO EXPLAINS THE PROCEDURES FOR APPLICATIONS THAT FAIL VALIDATION.

5.1 Validation Requirements for Certificate Applications

Upon receipt of a certificate application (per CPS § 4 – Certificate Application Procedures) GlobalSign shall perform all required validations as a prerequisite to certificate issuance (per CPS § 6 – Issuance of Certificates), as follows.

Confirm that

- the certificate applicant is the person identified in the request (in accordance with and only to the extent provided in the certificate class descriptions, *see* CPS § 2, and as further described below),
- the certificate applicant rightfully holds the private key corresponding to the public key to be listed in the certificate,
- the information to be listed in the certificate is accurate, except for nonverified subscriber information (NSI), and
- any agents who apply for a certificate listing the certificate applicant's public key (permissible for secure server certificates and object publishing certificates only) are duly authorised to make such a request.

Once a certificate is issued, GlobalSign shall have no continuing duty to monitor and investigate the accuracy of the information in a certificate, unless GlobalSign is notified in accordance with this CPS of that certificate's compromise.

Table 6 (Validation Requirements for Certificate Applications) highlights certain differences between the validation requirements for each certificate class. GlobalSign reserves the right to update these validation procedures to improve the validation process. Further details concerning validations are presented below. Updated validation procedures (when released) are presented in the GlobalSign repository at http://www.globalsign.net/repository and may also be obtained from GlobalSign, NV/SA, Kunstlaan/Avenue des Arts 1-2, B 4, 1210 Brussels, Belgium Attn. Legal department.

VALIDATION REQUIREMENTS	Class 1	Class 2	Class 3
PERSONAL PRESENCE	No	No	Yes – Before a (L)RA
PERSONAL INVESTIGATION (FOR INDIVIDUALS)	No	Yes – By a (L)RA	Yes –By a (L)RA
THIRD-PARTY CONFIRMATION OF BUSINESS ENTITIES	n/a	n/a	n/a
DOMAIN NAME CONFIRMATION OF BUSINESS ENTITIES	n/a	n/a	n/a

	secure server	object publishing

PERSONAL PRESENCE	No – Optional	No - Optional
PERSONAL INVESTIGATION (FOR INDIVIDUALS)	n/a	Yes – By a (L)RA
THIRD-PARTY CONFIRMATION OF BUSINESS ENTITIES	Yes – By a (L)RA	Yes – By a (L)RA
DOMAIN NAME CONFIRMATION OF BUSINESS ENTITIES	Yes – By a (L)RA	Yes – By a (L)RA

Table 6 – Validation Requirements for Certificate Applications

5.1.1 Personal Presence

In order to effect an appropriate binding between the applicant and the applicant's public key, individuals applying for Class 3 certificates must appear personally before a trusted entity (such as a LRA) to facilitate the confirmation of their identity. A personal presence requirement has many variables, including but not limited to specified identification documents.

5.1.2 Third-Party Confirmation of Business Entity Information

Where required, the third party confirms the business entity's name, address, and other registration information through comparison with third-party databases and through inquiry to the appropriate government entities. Confirmation of information of companies, banks, requires certain customised (and possibly localised) procedures focusing on specific business-related criteria (such as proper business registration). The third party also provides telephone numbers that are used for out-of-band communications with the business entity to confirm certain information (for example, to confirm an agent's position within the business entity or to confirm that the particular individual listed in the application is in fact the applicant). If its databases do not contain all the information required, the third party may undertake an investigation, if requested by GlobalSign, or the certificate applicant may be required to provide additional information and proof.

5.1.3 Domain Name Confirmation & Serial Number Assignment

GlobalSign shall have sole discretion regarding the assignment of relative distinguished names (RDNs) and certificate serial numbers appearing in the certificates they issue. GlobalSign shall use the Domain Name Service for resolving RDN assignment where appropriate. For information about Domain Name procedures and assurances, see for example **http://www.dns.be.**

5.2 Approval of Certificate Applications

Upon successful performance of all required validations of certificate application (in accordance with CPS § 5.1), GlobalSign shall approve the application. Approval is demonstrated by issuing a certificate according to CPS § 6 (Issuance of Certificates).

5.3 Rejection of Certificate Application

If a validation fails, GlobalSign shall reject the certificate application by promptly notifying the certificate applicant of the validation failure and providing the reason code (except where prohibited by law) for such failure. Such notice shall be communicated to the certificate applicant using the same method as was used to communicate the certificate application to GlobalSign or (L)RA). A person whose certificate application has been rejected may thereafter reapply.

6. ISSUANCE OF CERTIFICATES

THIS SECTION PRESENTS THE REQUIREMENTS FOR THE ISSUANCE OF CERTIFICATES. IT ALSO LISTS THE SPECIFIC REPRESENTATIONS ISSUING AUTHORITIES MAKE UPON ISSUING CERTIFICATES.

6.1 Certificates

Upon approving a certificate application (per CPS § 5), GlobalSign issues a certificate. The issuance of a certificate indicates a complete and final approval of the certificate application by GlobalSign. The certificate is deemed to be a valid certificate upon the subscriber's acceptance of it (*see* CPS § 7 regarding acceptance).

6.2 Consent by Subscriber for Issuance of Certificate by GlobalSign

GlobalSign shall not issue certificates without the certificate applicant's consent. Consent to issue is presumed from applicant's submission of an application notwithstanding the fact that acceptance of a certificate has not yet occurred.

6.3 Refusal to Issue a Certificate

GlobalSign may refuse to issue a certificate to any person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal.

6.4 GlobalSign Representations Upon Certificate Issuance

6.4.1 GlobalSign Representations to Subscriber

(i) Unless otherwise provided in this CPS or mutually agreed upon by both GlobalSign and the subscriber in an authenticated record, GlobalSign promises to the subscriber named in the certificate that

(a) there are no misrepresentations of fact in the certificate known to GlobalSign or originating from GlobalSign,

(b) there are no data transcription errors as received by GlobalSign from the certificate applicant resulting from a failure of GlobalSign to exercise reasonable care in creating the certificate, and

(c) the certificate meets all material requirements of this CPS.

(ii) Unless otherwise provided in this CPS or mutually agreed upon by both GlobalSign and the subscriber in an authenticated record, GlobalSign promises to the subscriber to make reasonable efforts, consistent with the terms of this CPS,

(a) to promptly revoke or suspend certificates in accordance with CPS § 9, and

(b) to notify subscribers of any facts known to it that materially affect the validity and reliability of the certificate it issued to such subscriber.

(iii) The obligations and representations in CPS §§ 6.4.1 (i) and (ii) are made and undertaken solely for the benefit of the subscriber and are not intended to benefit or be enforceable by any other party. GlobalSign makes reasonable efforts, for purposes of CPS § 6.4.1(ii), if its conduct substantially complies with this CPS and applicable law.

6.4.2 GlobalSign's Representations to Relying Parties

By issuing a certificate GlobalSign represents to all who reasonably rely on a digital signature verifiable by the public key listed in the certificate that consistent with this CPS:

(a) all information in or incorporated by reference within the certificate, except non-verified subscriber information (NSI), is accurate, and

(b) GlobalSign has complied with the CPS when issuing the certificate.

6.5 GlobalSign Representations Upon Publication

By publishing a certificate (*see* CPS § 7.5), GlobalSign certifies to the GlobalSign repository and to all who reasonably rely on the information contained in the certificate that it has issued the certificate to the subscriber and that the subscriber has accepted the certificate, as described in CPS § 7.1.

6.6 Time of Certificate Issuance

GlobalSign shall make reasonable efforts to confirm certificate application information and issue end-user subscriber certificates once all relevant information is received by GlobalSign within the following time periods:

	CLASS 1	**CLASS 2**	**CLASS 3**	**SECURE SERVER**	**OBJECT PUBLISHING**
Time Period	"Immediately" to 24 hours	"Immediately" to 3 business days	1-5 business days	1-5 business days	1-5 business days

Table 7 – Certificate Issuance Deadlines

6.7 Certificate Validity and Operational Periods

All certificates shall be considered valid upon issuance by GlobalSign and acceptance by the subscriber (*see* CPS § 7). The standard operational periods for the various classes of certificates are as follows, subject to earlier termination of the operational period due to suspension or revocation.

CERTIFICATE \ISSUED BY:	**CLASS 1**	**CLASS 2**	**CLASS 3**	**SECURE SERVER**	**OBJECT PUBLISHING**
CA to End-user/ Subscriber	30 days	1 year	1 year	1 year	1 year

Table 8 – Certificate Operational Periods

6.8 Restrictions on Issued but not Accepted Certificates

A subscriber must not create digital signatures using a private key corresponding to the public key listed in a certificate (or otherwise use such private key) if the foreseeable effect would be to induce or allow reliance upon a certificate which is invalid (because it has not been accepted).

7. ACCEPTANCE OF CERTIFICATES BY SUBSCRIBERS

THIS SECTION EXPLAINS THE REQUIREMENTS FOR CERTIFICATE ACCEPTANCE BY SUBSCRIBERS, THE REPRESENTATIONS MADE BY SUBSCRIBERS UPON ACCEPTANCE, SUBSCRIBERS' OBLIGATIONS TO PROTECT THEIR PRIVATE KEYS, AND PROCEDURES FOR THE PUBLICATION OF CERTIFICATES.

7.1 Certificate Acceptance

A subscriber is deemed to have accepted a certificate when, following communication of the application per CPS § 4.2, approval is manifested as described in Table 9.

CLASS	Means of Establishing Acceptance
CLASS 1	**INDIVIDUALS:** On-line: via the Web (https). The certificate applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate. E-mail (S/MIME): The certificate applicant submits a CSR to GlobalSign to accept the certificate. Upon completion of specified validation procedures, GlobalSign then sends the certificate to the E-mail address from which the certificate application originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate. **BUSINESS ENTITIES: N/A**
CLASS 2	**INDIVIDUALS:** On-line): Via the Web (https). The certificate applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate. E-mail (S/MIME): The certificate applicant submits a CSR to GlobalSign to accept the certificate. Upon completion of specified validation procedures, GlobalSign then sends the certificate to the E-mail address from which the certificate application originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate. **BUSINESS ENTITIES: N/A**
CLASS 3	**INDIVIDUALS:** On-line: Via the Web (https). The certificate applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate. E-mail (S/MIME): The certificate applicant submits a CSR to GlobalSign to accept the certificate. Upon completion of specified validation procedures, GlobalSign then sends the certificate to the E-mail address from which the certificate application originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate. **BUSINESS ENTITIES: N/A**
SECURE SERVER	**INDIVIDUALS: N/A** **BUSINESS ENTITIES:** On-line: Via the Web (https). The certificate applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate. E-mail (S/MIME): The certificate applicant submits a CSR to GlobalSign to accept the certificate. Upon completion of specified validation procedures, GlobalSign then sends the certificate to the E-mail address from which the certificate application originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a

	certificate or earlier notice of informational content to be included in the certificate.
OBJECT PUBLISHING	**INDIVIDUALS: N/A** **BUSINESS ENTITIES:** On-line: Via the Web (https). The certificate applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate. E-mail (S/MIME): The certificate applicant submits a CSR to GlobalSign to accept the certificate. Upon completion of specified validation procedures, GlobalSign then sends the certificate to the E-mail address from which the certificate application originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

Table 9 – Methods of Certificate Acceptance

7.2 Representations by Subscriber Upon Acceptance

By accepting a certificate issued by GlobalSign, the subscriber certifies to and agrees with GlobalSign and to all who reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber,

(i) each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired, suspended or revoked) at the time the digital signature is created,

(ii) no unauthorised person has ever had access to the subscriber's private key,

(iii) all representations made by the subscriber to GlobalSign regarding the information contained in the certificate are true,

(iv) all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and does not promptly notify GlobalSign of any material inaccuracies in such information as set forth in CPS § 6.1,

(v) the certificate is being used exclusively for authorised and legal purposes, consistent with this CPS, and

(vi) the subscriber is an end-user subscriber and not an CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as an CA or otherwise, unless expressly agreed in writing between subscriber and GlobalSign.

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT HE, SHE, OR IT AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT.

7.3 Subscriber Duty to Prevent Private Key Disclosure

By accepting a certificate, the subscriber assumes a duty to retain control of the subscriber's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure, modification, or unauthorised use.

7.4 Indemnity by Subscriber

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD GLOBALSIGN, AND THEIR AGENT(S) AND CONTRACTORS 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 GLOBALSIGN, AND THEIR AGENTS AND CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE, AND THAT ARISES FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE

AUTHORIZED BY THE SUBSCRIBER); (II) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE THE CA, GLOBALSIGN, OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; OR (III) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM, OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE OF THE SUBSCRIBER'S PRIVATE KEY.

When a certificate is issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify GlobalSign, and their agents and contractors pursuant to this subsection. The subscriber has a continuing duty to notify the issuer of any misrepresentations and omissions made by an agent.

7.5 Publication

Upon subscriber's acceptance of the certificate, and checking by GlobalSign, GlobalSign shall publish a copy of the certificate in the GlobalSign repository or in one or more other repositories, as determined by GlobalSign. Subscribers may publish their GlobalSign CPS certificates in other repositories.

8. USE OF CERTIFICATES

THIS SECTION ADDRESSES THE RIGHTS AND OBLIGATIONS OF THE ENTITIES WHOSE RIGHTS AND OBLIGATIONS ARE INTENDED TO BE CONTROLLED BY THIS CPS (*SEE* DEFINITION OF "PARTIES") REGARDING THE USE OF DIGITAL SIGNATURES AND DIGITALLY SIGNED MESSAGES CORRESPONDING TO GLOBALSIGN-ISSUED CERTIFICATES.

The parties (GlobalSign and the parties who are "users" of the certificate, *i.e.,* the subscriber and the relying parties), are hereby notified of the following rules governing the respective rights and obligations of the parties among themselves, which are also deemed to be agreed by the parties, effective (i) upon publication of this CPS in the case of GlobalSign; (ii) upon submission of an application for a certificate, in the case of an applicant or subscriber; and (iii) upon reliance of a certificate or a digital signature verifiable with reference to a public key listed in the certificate, in the case of a recipient of a certificate or a relying party.

8.1 Verification of Digital Signatures

Verification of a digital signature, is undertaken to determine that (i) the digital signature was created by the private key corresponding to the public key listed in the signer's certificate and that (ii) the associated message has not been altered since the digital signature was created.

Such verification shall be undertaken in a manner consistent with this CPS, as follows:

- **Establishing a certificate chain for the digital signature** – A digital signature shall be verified with regard to a successful confirmation of certificate chain.
- **Ensuring that the identified certificate chain is the most suitable for the digital signature** – It is possible to have more than one valid certificate chain leading from a given certificate to an acceptable root (such as through cross-certification among other possibilities). If there is more than one certificate chain to an acceptable root, the person verifying the digital signature may have various options in selecting and validating the certificate chain.
- **Checking the GlobalSign (or other) repository for revocation or suspension of certificates in the chain** – The recipient must determine if any of the certificates along the chain from the signer to an acceptable root within the PCS has been revoked or suspended, because a revocation or suspension has the effect of prematurely terminating the operational period during which verifiable digital signatures can be created. This may be ascertained in two different ways. The GlobalSign repository may be queried for the most up-to-date revocation status. Alternatively, CRLs may have been provided in the certificate chain. These CRLs may be used to determine the revocation status of certificates in the chain.
- **Delimiting data to which digital signatures are attached** – In order to verify a digital signature it is necessary to know precisely what data has been signed. In the case of public key cryptography standards (PKCS), a standard signed message format is specified to accurately denote the signed data.
- **Indicating digital signature time and date of creation** – In order for a digital signature to support non-repudiation, the data to which the corresponding digital signature is attached must include, or reference, a time stamp. The time stamp shall reflect the time at which date and time the digital signature is affixed.
- **Establishing the assurances intended by its signer** – Various technical means may be used to determine the purpose (or meaning) of the digital signature intended by its signer. In formal protocols (such as EDI), digital signatures are classified as specified security services with defined semantics so as to convey their precise meaning. The verifier should also determine whether the certificate is normal or provisional.
- **Ensuring that all certificates in the chain authorise use of an end-user subscriber private key** – GlobalSign may limit the purposes for which a private key corresponding to a certificate it issues may be used. Such limitations are indicated or incorporated by reference in the certificate and provide a means to warn recipients of situations for which reliance upon the certificate would not be considered reasonable. Persons validating certificates must inspect certificate contents for such warnings and

limitations to ensure that no certificate in the chain denies appropriate use of an end-user subscriber certificate.

- **Confirmation of a certificate chain** – Each CA is certified by a superior CA (except for the root, which has a self-signed public key) and thus inherits the trust associated with its superior CA. Each CA is presumed to be as trustworthy as its superior CA. Confirmation of a certificate chain is the process of validating a certificate chain and subsequently validating an end-user subscriber certificate.

8.2 Effect of Validating an End-User Subscriber Certificate

A digital signature can be binding against its maker if the law defines so and if it (i) was created during the operational period of a valid certificate, (ii) such digital signature can be properly verified by confirmation of certificate chain (iii) the relying party has no knowledge or notice of a breach of the requirements of this CPS by the signer and (iv) the relying party has complied with all requirements of this CPS.

8.3 Procedures upon Failure of Digital Signature Verification

A person relying on an unverifiable digital signature assumes all risks with regard to it and is not entitled to any presumption that the digital signature is effective as the signature of the subscriber under CPS §§ 8.4-8.6.

8.4 Reliance on Digital Signatures

A recipient of a message signed by a digital signature of the subscriber may rely upon that digital signature as binding against the subscriber if:

(i) the digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate chain, and

(ii) such reliance is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be reasonable.

Additionally, the verifier should consider the class of certificate. The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the verifier.

8.5 Writings

When admitted by law, a message bearing a digital signature verified by the public key listed in a valid certificate is as valid, effective, and enforceable as if the message had been written and signed on paper.

8.6 Signatures

Where a rule of law or applicable practice requires a signature or provides for certain consequences in the absence of a signature, that rule can be satisfied in relation to a message by a digital signature affixed by a signer with the intention of signing a message and subsequently verified by reference to the public key listed in a valid certificate, if admitted by law.

8.7 Security Measures

Any person using or relying upon a GlobalSign PCS-issued certificate in conjunction with a message shall apply reasonable security measures to the message to provide message authentication and, as required, to support data confidentiality.

8.8 Issuing Certificates

Only CAs accredited by GlobalSign may issue GlobalSign certificates. The accreditation conditions are available at legal@globalsign.net.

8.9 Security of digital signatures

Any person using digital certificates shall need to sign again signed data after a certain time because of security reasons due to the evolution of the technology of digital certificates. GlobalSign shall periodically publish information about this in the GlobalSign repository.

9. CERTIFICATE SUSPENSION AND REVOCATION

THIS SECTION EXPLAINS THE CIRCUMSTANCES UNDER WHICH A CERTIFICATE MAY (OR MUST) BE SUSPENDED OR REVOKED. IT ALSO DETAILS THE PROCEDURES FOR SUSPENDING, REVOKING, AND REINSTATING CERTIFICATES.

9.1 Reasons for Suspension or Revocation, Generally

A certificate shall be suspended or revoked if

- there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject,
- the certificate's subject (whether GlobalSign or a subscriber) has breached a material obligation under this CPS, or
- 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.

9.2 Suspension or Revocation of a GlobalSign Certificate

GlobalSign must make a reasonable effort to suspend or revoke a certificate, if it determines any of the following:

- a material fact represented in the certificate is known or reasonably believed by GlobalSign to be false,
- a material prerequisite to certificate issuance was not satisfied
- the private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability, or
- the certificate's subject has breached a material obligation under this CPS.

9.3 Termination of a Suspension of a GlobalSign Certificate

GlobalSign shall terminate a certificate suspension (thereby reinstating the certificate), if (i) the subscriber requests it and GlobalSign confirms his or her identity and (ii) GlobalSign determines that the reasons for the suspension were unfounded.

9.4 Revocation at Subscriber's Request

GlobalSign must revoke a certificate upon the subscriber's request once it has confirmed that the person requesting the revocation is in fact the subscriber.

9.5 Revocation Due to Faulty Issuance

GlobalSign shall revoke a certificate promptly upon discovering and confirming that it was not issued in accordance with the procedures required by this CPS. A certificate may be suspended while GlobalSign investigates to confirm grounds for revocation. Table 10 details revocation prerequisites.

	PREREQUISITES FOR GLOBALSIGN REVOKING A CERTIFICATE
CA	• The request must be done in the form of an authenticated record from the subscriber or its agent or by means of a challenge phrase.

Table 10 – Revocation Prerequisites

9.6 Notice and Confirmation upon Suspension or Revocation

Upon suspending or revoking a certificate, GlobalSign must publish notice of the suspension or revocation in the GlobalSign repository. GlobalSign may publish one or more of the following:

- a listing of revoked (and suspended) certificates available through a secure channel,
- a certificate revocation list (CRL) designating both revoked and suspended certificates,

GlobalSign may also provide the following suspension and revocation notification services upon request and payment of associated fees by the requester:

- confirming that a certificate has been suspended or revoked, if asked to do so by a recipient of a digitally signed message, originated by the subject of that certificate.

9.7 Effect of Suspension or Revocation

9.7.1 On Certificates

During suspension, or permanently upon revocation of a subscriber's certificate, that certificate's operational period shall immediately be considered terminated.

9.7.2 On Underlying Obligations

Suspension or revocation of a certificate shall not affect any underlying contractual obligations created or communicated under this CPS.

9.8 Safeguarding of Private Key upon Suspension or Revocation

Private keys corresponding to public keys contained in suspended or revoked certificates shall be safeguarded by the subscriber in a trustworthy manner throughout the period of suspension and, upon revocation, unless destroyed.

10. CERTIFICATE EXPIRATION

THIS SECTION DESCRIBES PARTIES' OBLIGATIONS REGARDING CERTIFICATE EXPIRATION. THIS IS DISTINCT FROM CERTIFICATE SUSPENSION AND REVOCATION (*SEE* CPS § 9). CERTIFICATE VALIDITY AND OPERATIONAL PERIODS ARE ADDRESSED IN CPS § 6.7.

10.1 Notice Prior to Expiration

GlobalSign will make a reasonable effort to notify subscribers thirty (30) days before the expiration date (except Class 1), via E-mail, of the impending expiration of their certificates. Such notice is intended solely for the convenience of the subscriber in the re-enrollment or renewal process, whichever is applicable.

10.2 Effect of Certificate Expiration on Underlying Obligations

Expiration of a certificate shall not affect the validity of any underlying contractual obligations created or communicated under this CPS.

10.3 Re-enrolment and Subscriber Renewal

Subscriber renewal and re-enrolment shall be initiated as follows:

Class 1	Class 2	Class 3	Secure server and object publishing
Same process as initial application.	Signed request for renewal or challenge phrase	Signed request for renewal	Signed request for renewal

Table 11 – Renewal and Re-Enrollment Requirements

Requirements for renewal and re-enrolment are subject to change at GlobalSign's discretion. Up-to-date requirements for re-enrolment and renewal are accessible (when available) from the GlobalSign repository at https://www.globalsign.net/repository

11. OBLIGATIONS OF GLOBALSIGN, AND LIMITATIONS UPON SUCH OBLIGATIONS

THIS SECTION SUMMARISES AND PROVIDES REFERENCES TO THE WARRANTIES AND PROMISES MADE BY GLOBALSIGN AND PRESENTS DISCLAIMERS AND LIMITATIONS UPON SUCH OBLIGATIONS.

11.1 Limited Warranties and Other Obligations

GlobalSign (to the extent specified in the referenced CPS sections) warrant and promise to

- provide the infrastructure and certification services, including the establishment and operation of the GlobalSign repository, as delineated in CPS § 2 (GlobalSign Certification Infrastructure),
- provide the controls and foundation for PKI, including CA key generation, key protection, and secret sharing procedures, presented in CPS § 3 (Foundation for Certification Operations),
- perform the application validation procedures for the indicated class of certificate as set forth in CPS § 5 (Validation of Certificate Applications),
- issue certificates in accordance with CPS § 6 and honour the various representations to subscribers and to relying parties presented in CPS § 6.5 (CA's Representations Upon Certificate Issuance),
- publish accepted certificates in accordance with CPS § 6.6 (GlobalSign's Representations Upon Publication) and CPS § 7.5 (Publication),
- perform the obligations of a CA and support the rights of the subscribers and relying parties who use certificates in accordance with CPS § 8 (Use of Certificates),
- revoke certificates as required by CPS § 9 (Certificate Revocation),
- provide for the expiration, re-enrollment, and renewal of certificates as stated in CPS § 10 (Certificate Expiration), and
- comply with the provisions contained in CPS § 12 (Miscellaneous Provisions).

Additionally, GlobalSign warrant that their own private keys are not compromised unless they provide notice to the contrary via the GlobalSign repository.

GLOBALSIGN MAKES NO OTHER WARRANTIES AND HAS NO FURTHER OBLIGATIONS UNDER THIS CPS.

11.2 Disclaimers and Limitations on Obligations of GlobalSign

EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING (CPS § 11.1), GLOBALSIGN DISCLAIMS ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF UNVERIFIED INFORMATION PROVIDED.

Except as expressly stated in the foregoing CPS § 11.1, GlobalSign

- does not warrant the accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of GlobalSign,
- does not warrant the accuracy, authenticity, completeness or fitness of any information contained in class 1 certificates,
- shall not incur liability for representations of information contained in a certificate, provided the certificate content complies with this CPS,
- shall not warrant the legal validity of a digital signature because this is determined exclusively by law,

- does not warrant "non-repudiation" of any certificate or message (because non-repudiation is determined exclusively by law and the applicable dispute resolution mechanism), and
- does not warrant any software.

11.3 Exclusion of Certain Elements of Damages

IN NO EVENT (EXCEPT FOR FRAUD OR WILFULL MISCONDUCT) SHALL GLOBALSIGN BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EXCEPT FOR DAMAGES DUE TO RELIANCE (IN ACCORDANCE WITH THIS CPS) ON THE VERIFIED INFORMATION IN A CLASS 2, CLASS 3, SECURE SERVER OR OBJECT PUBLISHING CERTIFICATE.

GLOBALSIGN WILL NOT BE LIABLE IN THIS CASE IF THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILFULL MIDCONDUCT OF THE APPLICANT.

11.4 Damage and Loss Limitations

IN NO EVENT (EXCEPT FOR FRAUD OR WILFULL MISCONDUCT) WILL THE LIABILITY OF GLOBALSIGN TO ALL PARTIES (INCLUDING WITHOUT LIMITATION A SUBSCRIBER, AN APPLICANT, A RECIPIENT, OR A RELYING PARTY) EXCEED THE APPLICABLE LIABILITY CAP FOR SUCH CERTIFICATE SET FORTH IN TABLE 12, BELOW.

THE LIABILITY OF GLOBALSIGN TO ANY AND ALL PERSONS CONCERNING A SPECIFIC CERTIFICATE SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED THE FOLLOWING, FOR THE AGGREGATE OF ALL DIGITAL SIGNATURES AND TRANSACTIONS RELATED TO SUCH CERTIFICATE:

	LIABILITY CAPS
CLASS 1	0 BEF
CLASS 2	100.000 BEF
CLASS 3	1.500.000 BEF
SECURE SERVER	1.500.000 BEF
OBJECT PUBLISHING	1.500.000 BEF

Table 12 - Liability Caps

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, consequential, exemplary, or incidental damages incurred by any person, including without limitation a subscriber, an applicant, a recipient, or a relying party, that are caused by reliance on the verified information in a class 2, class 3, secure server or object publishing certificate GlobalSign issues, manages, uses, suspends or revokes, or such a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim within the limits of the law. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall GlobalSign be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

11.5 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

11.6 No Fiduciary Relationship

GLOBALSIGN IS NOT THE AGENT, FIDUCIARY, TRUSTEE, OR OTHER REPRESENTATIVE OF SUBSCRIBERS OR RELYING PARTIES.

The relationship between GlobalSign and subscribers and that between GlobalSign and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind GlobalSign, by contract or otherwise, to any obligation. GlobalSign shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

11.7 Hazardous Activities

GlobalSign's public certification services are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

12. MISCELLANEOUS PROVISIONS

THIS SECTION PRESENTS GENERAL TERMS AND CONDITIONS OF THIS CPS THAT ARE NOT COVERED IN THE OTHER SECTIONS.

12.1 Conflict of Provisions

In the event of a conflict between this CPS and other rules, guidelines, or contracts, the subscriber shall be bound by the provisions of this CPS, except as to other contracts either (i) predating the first public release of the CPS or (ii) expressly superseding this CPS for which such contract shall govern as to the parties thereto, and except to the extent that the provisions of this CPS are prohibited by law.

12.2 Compliance with Export Laws and Regulations

Export of certain software used in conjunction with GlobalSign's PCS may require the approval of appropriate government authorities. The parties shall conform to applicable export laws and regulations.

12.3 Governing Law

The Belgian law shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions. This choice of law is made to ensure uniform procedures and interpretation for all users, no matter where they reside or use their certificates.

12.4 Dispute Resolution

12.4.1 Notification Among Parties to a Dispute

Before invoking arbitration (as detailed below) with respect to a dispute involving any aspect of this CPS or a certificate issued by GlobalSign, aggrieved persons shall notify GlobalSign, and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

12.4.2 Arbitration

If the dispute is not resolved within ten (10) days after initial notice pursuant to CPS Sect. 12.4.1, then parties will submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code. There will be 3 arbitrators. Each party will chose one arbitrator. The third arbitrator will be chosen by the two parties in agreement. The place of the arbitration will be determined by mutual agreement. The cost and its division will be determined by the arbitrators.

12.5 Successors and Assigns

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with CPS § 3.21, concerning termination or cessation of CA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

12.6 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of GlobalSign may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

12.7 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so as best to reasonably effect the intent of its parties.

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS CPS THAT PROVIDES FOR A LIMITATION OF LCABILITY, DISCLAIMER OF OR LIMITATION UPON ANY WARRANTIES OR OTHER OBLIGATIONS, OR EXCLUSION OF DAMAGES IS INTENDED TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND IS TO BE ENFORCED AS SUCH.

12.8 Interpretation

Unless otherwise provided, this CPS shall be interpreted consistently with what is commercially reasonable under the circumstances. In interpreting this CPS, regard is to be given to its international scope and application, to the benefits in promoting uniformity in its application, and to the observance of good faith.

12.9 No Waiver

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

12.10 Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgement of receipt from the recipient. Such acknowledgement must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To GlobalSign: GlobalSign, NV/SA.
Kunstlaan/Avenue des Arts 1-2, B4
Bruxelles 1210
Attn: Legal department

12.11 Headings and Appendices of this CPS

The headings, subheadings, and other captions in this CPS are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS. The appendices, including the definitions to this CPS, are for all purposes an integral and binding part of the CPS.

12.12 Change of Subscriber Information on File with GlobalSign; Change to CPS

Any subscriber may change certain information about itself on file with GlobalSign that does not appear within its certificate (typically, information provided in the certificate application) upon giving thirty (30) days notice in accordance with CPS § 12.10 (Notice). Such change in information shall be effective after such thirty (30) day period.

GlobalSign may amend or modify this CPS from time to time (prospectively and not retroactively). Each change shall become effective fifteen (15) days after GlobalSign publishes a proposal for the change in the GlobalSign repository unless (i) GlobalSign has published a notice of withdrawal of the proposed change in the GlobalSign repository prior to the end of such fifteen (15) day period, or (ii) failure by GlobalSign to make the proposed change may result in a compromise of the PCS or any portion of it, in which case, the proposed change is effective upon publication in the GlobalSign repository. A subscriber's decision not to request revocation of his, her, or its certificate following the publication of a proposed change shall constitute agreement to the change.

12.13 Property Interests in Security Materials

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

- **Certificates:** Certificates are the personal property of their respective CA. Permission is hereby granted to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates shall not be published in any publicly accessible repository or directory without the express written permission of GlobalSign. This restriction is intended, in part, to protect the privacy of subscribers against unauthorised republication of their certificates. Questions concerning this copyright notice should be sent to GlobalSign as listed in CPS § 12.10 (Notice), or to legal@globalsign.net.
- **CPS:** This CPS is the personal property of GlobalSign, NV/SA
- **Private keys:** Private keys are the personal property of the subscribers who rightfully use or are capable of using them, regardless of the physical medium within which they are stored and protected.
- **Public keys:** Public keys are the personal property of subscribers, regardless of the physical medium within which they are stored and protected.
- **Secret shares of private keys:** Secret shares of a CA's private key are the personal property of the applicable CA.

12.14 Infringement and Other Damaging Material

Certificate applicants (and, upon acceptance, subscribers) represent and warrant that their submission (to GlobalSign) and use of a domain and distinguished name (and all other certificate application information) does not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Certificate applicants (and, upon acceptance, subscribers) shall defend, indemnify, and hold GlobalSign harmless for any loss or damage resulting from any such interference or infringement.

GlobalSign shall not be responsible for non-verified subscriber information (NSI) submitted to GlobalSign, or the GlobalSign directory or otherwise submitted for inclusion in a certificate. In particular, subscribers shall be solely responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed. Because laws regarding the transmission and availability of information content are constantly changing and vary widely, certificate applicants' and subscribers' responsibilities are determined not only by laws in existence at the time GlobalSign issues a certificate to a certificate applicant but also by any laws that may be enacted after such date. Certificate applicants and subscribers should be aware that there are many laws regarding the transmission of data, especially data that is encrypted or involves encryption algorithms, and that these laws may vary dramatically from country to country. Further, it is generally not possible to limit the distribution of content on the Internet or certain other networks based on the locality of the user/viewer, and this may require certificate applicants and subscribers to comply with the laws of each jurisdiction in which the content may be viewed or used.

Certificate applicants and subscribers will not submit to GlobalSign, or the GlobalSign directory any materials that contain statements that (i) are libellous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

12.15 Fees

GlobalSign may charge subscribers fees for their use of GlobalSign's services. A current schedule of such fees is available from the GlobalSign web-site at http://www.globalsign.net/products . Such fees are subject to change seven (7) days following their posting at the GlobalSign web-site.

12.16 Choice of Cryptographic Methods

All persons acknowledge that they are solely responsible for and have exercised independent judgement in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques.

12.17 Survival

The obligations and restrictions contained within CPS § 3.7 (Audit), 3.11 (Confidential Information), CPS § 11 (Obligations of GlobalSign, and Limitations Upon Such Obligations), and CPS § 12 (Miscellaneous Provisions) shall survive the termination of this CPS.

***

13. APPENDICES

13.1 Definitions

A-B

ACCEPT (A CERTIFICATE)

To demonstrate approval of a certificate by a certificate applicant while knowing or having notice of its informational contents, in accordance with the CPS.

ACCREDITATION

A formal declaration by a GlobalSign–designated approving authority that a particular information system, professional or other employee or contractor, or organization is approved to perform certain duties and to operate in a specific security mode, using a prescribed set of safeguards.

AFFIRM / AFFIRMATION

To state or indicate by conduct that data is correct or information is true.

ALIAS

A pseudonym.

APPLICANT (*SEE* CERTIFICATE APPLICANT)

ARCHIVE

To store records and associated journals for a given period of time for security, backup, or auditing purposes.

ASSURANCES

Statements or conduct intended to convey a general intention, supported by a good-faith effort, to provide and maintain a specified service by an CA. "Assurances" does not necessarily imply a guarantee that the services will be performed fully and satisfactorily. Assurances are distinct from insurance, promises, guarantees, and warranties, unless otherwise expressly indicated.

AUDIT

A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

AUTHENTICATE (*SEE* AUTHENTICATION)

AUTHENTICATED RECORD

A signed document with appropriate assurances of authentication or a message with a digital signature verified by a valid Class 3 certificate by a relying party. However, for suspension and revocation notification purposes, the digital signature contained in such notification message must have been created by the private key corresponding to the public key contained in the certificate for the applicable certificate class.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (*Cf.*, **VERIFY (**a **DIGITAL SIGNATURE)**)

AUTHENTICODE (*SEE* MICROSOFT AUTHENTICODE; SOFTWARE VALIDATION)

AUTHORIZATION

The granting of rights, including the ability to access specific information or resources.

AVAILABILITY

The extent to which information or processes are reasonably accessible and usable, upon demand, by an authorized entity, allowing authorized access to resources and timely performance of time-critical operations.

BINDING

An affirmation by an CA (or its LRA) of the relationship between a named entity and its public key.

C

CERTIFICATE (PUBLIC KEY CERTIFICATE)

A message (*see* definition for **MESSAGE**) that, at least, states a name or identifies the CA, identifies the subscriber, contains the subscriber's public key, identifies the certificate's operational period, contains a certificate serial number, and is digitally signed by the CA. All references to a "Class [1, 2, or 3] certificate" or to a "certificate" without a modifying adjective are intended as references to normal certificates, unless the context requires otherwise. References to a certificate refer exclusively to certificates issued by an CA. (*Cf.,* **NORMAL CERTIFICATE**)

CERTIFICATE APPLICANT

A person or authorized agent that requests the issuance of a public key certificate by an CA. (*Cf.,* **CA APPLICANT; SUBSCRIBER**)

CERTIFICATE APPLICATION

A request from a certificate applicant (or authorized agent) to an CA for the issuance of a certificate. (*Cf.,* **CERTIFICATE APPLICANT; CERTIFICATE SIGNING REQUEST**)

CERTIFICATE CHAIN

An ordered list of certificates containing an end-user subscriber certificate and CA certificates (*See* **VALID CERTIFICATE**)

CERTIFICATE EXPIRATION

The time and date specified in the certificate when the operational period ends, without regard to any earlier suspension or revocation.

CERTIFICATE EXTENSION

An extension field to a certificate which may convey additional information about the public key being certified, the certified subscriber, the certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594-8:1995 (X.509). Custom extensions can also be defined by communities of interest.

CERTIFICATE HIERARCHY

A PCS domain of CAs, each categorised with respect to its role in a "tree structure" of subordinate CAs. An CA issues and manages certificates for end-user subscribers and/or for one or more CAs at the next level. Note: an CA in a trust hierarchy must observe uniform practices addressing issues such as naming, maximum number of levels, etc., to assure integrity of the domain and thereby ensure uniform accountability, auditability, and management through the use of trustworthy operational processes.

CERTIFICATE ISSUANCE

The actions performed by an CA in creating a certificate and notifying the certificate applicant (anticipated to become a subscriber) listed in the certificate of its contents.

CERTIFICATE MANAGEMENT

Certificate management includes, but is not limited to, storage, dissemination, publication, revocation, and suspension of certificates. An CA undertakes certificate management functions by

serving as a registration authority for subscriber certificates. An CA designates issued and accepted certificates as valid by publication.

CERTIFICATE OF AUTHENTICITY

A document issued by an authorized official of the jurisdiction in which an acknowledgment by a notary was taken, such as the secretary of state of a state (U.S.) to authenticate the status of a notary.

CERTIFICATE REVOCATION (*SEE* REVOKE A CERTIFICATE)

CERTIFICATE REVOCATION LIST (CRL)

A periodically (or exigently) issued list, digitally signed by an CA, of identified certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked certificates' serial numbers, and the specific times and reasons for suspension and revocation.

CERTIFICATE SERIAL NUMBER

A value that unambiguously identifies a certificate generated by an CA.

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable form of a certificate application. (*Cf.,* **CERTIFICATE APPLICATION**)

CERTIFICATE SUSPENSION (*SEE* SUSPEND A CERTIFICATE)

CERTIFICATION / CERTIFY

The process of issuing a certificate by an CA.

CERTIFICATION AUTHORITY (CA)

GlobalSign that issues, suspends, or revokes a certificate. CAs are identified by a distinguished name on all certificates and CRLs they issue.GlobalSign is a CA. (*Cf.,* **REGISTRATION AUTHORITY; TRUSTED THIRD PARTY**)

CERTIFICATION PRACTICE STATEMENT (CPS)

This document, as revised from time to time (representing GlobalSign's statement of the practices GlobalSign employs in issuing certificates).

CERTIFIER (*SEE* CA)

CHALLENGE PHRASE

A set of numbers and/or letters that are chosen by a certificate applicant, communicated to the CA with a certificate application, and used by the CA to authenticate the subscriber for various purposes as required by the CPS. A challenge phrase is also used by a secret share holder to authenticate himself, herself, or itself to a secret share issuer.

CLASS [1, 2, OR 3] CERTIFICATE

A certificate of a specified level of trust. (*See* CPS § 2.2)

COMMERCIAL REASONABLENESS

In the context of electronic commerce, the implementation and use of technology, controls, and administrative and operational procedures that reasonably ensure system and message trustworthiness.

COMMERCIAL SOFTWARE PUBLISHER CERTIFICATE

A Class 3 Highest Level certificate that is issued to organizations only and is used for software validation. (*Cf.,* **INDIVIDUAL SOFTWARE PUBLISHER CERTIFICATE; SOFTWARE VALIDATION**)

COMMON KEY

Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case common key refers to this last share. It is not assumed to be secret as it is not continually in an individual's possession.

COMPROMISE

A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. (*Cf.,* **DATA INTEGRITY**)

CONFIDENTIALITY

The condition in which sensitive data is kept secret and disclosed only to authorized parties.

CONFIRM

To ascertain through appropriate inquiry and investigation. (*Cf.,* **AUTHENTICATE; VERIFY A DIGITAL SIGNATURE**)

CONFIRMATION OF CERTIFICATE CHAIN

The process of validating a certificate chain and subsequently validating an end-user subscriber certificate.

CONTENT INTEGRITY SERVICES

Content integrity services provide certificates to software publishers who desire to digitally sign their software publications to facilitate their customers' (end-users') ability to undertake software validation.

CONTROLS

Measures taken to ensure the integrity and quality of a process.

CORRESPOND

To belong to the same key pair. (*See also* **PUBLIC KEY; PRIVATE KEY**)

CROSS-CERTIFICATION

A condition in which either or both GlobalSign and a non-GlobalSign certificate issuing entity (representing another certification domain) issues a certificate having the other as the subject of that certificate.

CRYPTOGRAPHIC ALGORITHM

A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

CRYPTOGRAPHY (*CF.*, PUBLIC KEY CRYPTOGRAPHY)

(i) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

(ii) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorised uses.

CRYPTOMODULE

A trustworthy implementation of a crypto system which safely performs encryption and decryption of data.

D

DATA

Programs, files, and other information stored in, communicated, or processed by a computer.

DATABASE

A set of related information created, stored, or manipulated by a computerised management information system.

DATA CONFIDENTIALITY (*SEE* CONFIDENTIALITY)

DATA INTEGRITY
A condition in which data has not been altered or destroyed in an unauthorized manner. (*See also* **THREAT; *cf.*, COMPROMISE**)

DENIAL OF SERVICE (*SEE* AVAILABILITY)
Name for a certificate.

DIGITAL SIGNATURE
A transformation of a message using an asymmetric cryptosystem 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 message has been altered since the transformation was made.

DIRECTORY (*CF.*, REPOSITORY)

DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context. (*e.g.*, countryName=US, state=California, organizationName=Electronic Inc., commonName=JohnDoe).

DOCUMENT
A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information. (*Cf.*, **MESSAGE; RECORD**)

E-F

ELECTRONIC MAIL ("E-MAIL")
Messages sent, received or forwarded in digital form via a computer-based communication mechanism.

ENCRYPTION
The process of transforming plaintext data into an unintelligible form (ciphertext) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

END-USER SUBSCRIBER
A subscriber which is not also an CA.

ENHANCED NAMING
The use of an extended organization field (OU=) in an X.509 v3 certificate.

ENROLLMENT
The process of a certificate applicant's applying for a certificate.

ENTITY (*SEE* PERSON)

EXTENSIONS
Extension fields in X.509 v3 certificates. (*See* **X.509**)

FILE TRANSFER PROTOCOL (FTP)
The application protocol that offers file system access from the Internet suite of protocols.

FTP (*SEE* FILE TRANSFER PROTOCOL)

G–H

GENERATE A KEY PAIR

A trustworthy process of creating 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.

GLOBALSIGN NAMING AUTHORITY

A GlobalSign registration authority that establishes and enforces controls over and has decision-making authority regarding the issuance of relative distinguished names for all CAs (but not for end-user subscribers). (*Cf.*, **NAMING AUTHORITY**).

GLOBALSIGN PUBLIC CERTIFICATION SERVICES (PCS)

The certification system provided by GlobalSign and any GlobalSign-authorized CAs described in this CPS.

GLOBALSIGN QUALIFIER

A data syntax facilitating the representation of a set of values which restrict the meaning of the GlobalSign CPS. The qualifier value augments the standard certificate policy extension present in all certificates according to the rules defined by X.509 for that extension type.

GLOBALSIGN SECURITY PROCEDURES (BSP)

The comprehensive document describing GlobalSign's internal security techniques and procedures. Note: for security reasons, GlobalSign cannot disclose the BSP for external review or publication.

HASH (HASH FUNCTION)

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that

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

I

IDENTIFICATION / IDENTIFY

The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of certificates.

IDENTITY

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

INCORPORATE BY REFERENCE

To make one message a part of another message by identifying the message to be incorporated, with information that enables the receiving party 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 to the extent permitted by law.

INDIVIDUAL SOFTWARE PUBLISHER CERTIFICATE

A Class 2 certificate that is issued to individuals only and is used for software validation. (*Cf.*, **COMMERCIAL SOFTWARE PUBLISHER CERTIFICATE; SOFTWARE VALIDATION**)

INTEGRITY (*SEE* DATA INTEGRITY)

ISSUING A CERTIFICATE (*SEE* CERTIFICATE ISSUANCE)

ISSUER (*SEE* ISSUING AUTHORITY)

J-L

KEY GENERATION

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

KEY PAIR

A private key and its corresponding public key. The public key can verify a digital signature created by using the corresponding private key. In addition, depending upon the type of algorithm implemented, key pair components can also encrypt and decrypt information for confidentiality purposes, in which case a private key uniquely can reveal information encrypted by using the corresponding public key.

LOCAL REGISTRATION AUTHORITY (LRA)

An entity appointed by an CA to assist other entities in applying for certificates, revoking (or where authorised, suspending) their certificates, or both and also approving such applications. An LRA is not the agent of a certificate applicant. An LRA may not delegate the authority to approve certificate applications.

M-N

MESSAGE

A digital representation of information; a computer-based record. A subset of **RECORD**. (*Cf.,* **MESSAGE; RECORD**)

MESSAGE INTEGRITY (*SEE* INTEGRITY)

MICROSOFT AUTHENTICODE (*SEE* SOFTWARE VALIDATION)

NAME

A set of identifying attributes purported to describe an entity of a certain type.

NAMING

Naming is the assignment of descriptive identifiers to objects of a particular type by an authority which follows specific issuing procedures and maintains specific records pertinent to an identified registration process. (*Cf.,* **NAMING AUTHORITY; GLOBALSIGN NAMING AUTHORITY**)

NAMING AUTHORITY

A body which executes naming policy and procedures and has control over the registration and assignment of primitive (basic) names to objects of a particular class. (*Cf.,* **NAMING; GLOBALSIGN NAMING AUTHORITY**)

NON-REPUDIATION

Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of non-repudiation. By way of illustration, a digital signature verified pursuant to this CPS can provide proof in support of a determination of non-repudiation by a trier of fact, but does not by itself constitute non-repudiation.

NON-VERIFIED SUBSCRIBER INFORMATION (NSI)

Information submitted by a certificate applicant to an CA, and included within a certificate, which has not been confirmed by the CA and for which the CA provides no assurances other than that

the information was submitted by the certificate applicant. Information such as titles, professional degrees, and accreditation are considered NSI unless otherwise indicated.

NON-GLOBALSIGN CA
A CA that is not owned or operated by GlobalSign. (*See* CPS § 3.1; *Cf.,* **CA**)

NORMAL CERTIFICATE (*SEE* CERTIFICATE)

NOTARY
A natural person authorised to perform notarial services such as taking acknowledgements, administering oaths or affirmations, witnessing or attesting signatures, and noting protests of negotiable instruments.

NOTICE
The result of notification in accordance with this CPS. (*See* CPS § 12.10)

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

O-P

ON-LINE
Communications that provide a real-time connection to the GlobalSign PCS.

OPERATIONAL CERTIFICATE
A certificate which is within its operational period at the present date and time or at a different specified date and time, depending on the context.

OPERATIONAL PERIOD
The period starting with the date and time a certificate is issued (or on a later date and time certain if stated in the certificate) and ending with the date and time on which the certificate expires or is earlier suspended or revoked.

ORGANISATION
An entity with which a user is affiliated. An organisation may also be a user.

ORIGINATOR
A person by whom (or on whose behalf) a data message is purported to have been generated, stored, or communicated. It does not include a person acting as an intermediary.

PARTIES
The entities whose rights and obligations are intended to be controlled by this CPS. These entities may include certificate applicants, CAs, subscribers, and relying parties. (*See* **USERS; CAS; RELYING PARTY**)

PASSWORD (PASS PHRASE; PIN NUMBER)
Confidential authentication information, usually composed of a string of characters used to provide access to a computer resource.

PC CARD (*SEE ALSO* SMART CARD)
A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

PERSON
A human being or an organization (or a device under the control of a human being or organization) capable of signing or verifying a message, either legally or as a matter of fact. (A synonym of **ENTITY**.)

PERSONAL PRESENCE

The act of appearing (physically rather than virtually or figuratively) before an LRA or its designee and proving one's identity as a prerequisite to certificate issuance under certain circumstances.

PKI HIERARCHY

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

PLEDGE (*SEE* SOFTWARE PUBLISHER'S PLEDGE)

PRIVATE KEY

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key. (*See also* **PUBLIC KEY CRYPTOGRAPHY; PUBLIC KEY**)

PUBLIC CERTIFICATION SERVICES (*SEE* GLOBALSIGN PUBLIC CERTIFICATION SERVICES)

PUBLIC KEY

A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files which can then be decrypted with the corresponding private key. (*See also* **PUBLIC KEY CRYPTOGRAPHY; PRIVATE KEY**)

PUBLIC KEY CERTIFICATE (*SEE* CERTIFICATE)

PUBLIC KEY CRYPTOGRAPHY (*CF.*, CRYPTOGRAPHY)

A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. The PKI consists of systems which collaborate to provide and implement the PCS and possibly other related services.

PUBLIC/PRIVATE KEY PAIR (*SEE* PUBLIC KEY; PRIVATE KEY; KEY PAIR)

PUBLISH / PUBLICATION

To record or file information in the GlobalSign repository and optionally in one or more other repositories in order to disclose and make publicly available such information in a manner that is consistent with this CPS and applicable law.

Q-R

QUALIFIER (*SEE* GLOBALSIGN QUALIFIER)

RECIPIENT (OF A DIGITAL SIGNATURE)

A person who receives a digital signature and who is in a position to rely on it, whether or not such reliance occurs. (*Cf.,* **RELYING PARTY**)

RECORD

Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term "record" is a superset of the two terms "document" and "message". (*Cf.*, **DOCUMENT; MESSAGE**)

RE-ENROLLMENT (*CF.*, RENEWAL)

REGISTERED STRING

A class of object subject to registration and recording procedures which demonstrates the value is unambiguous within the records of the registration authority. The type of value recorded is a string of characters.

REGISTRATION AUTHORITY

An entity trusted to register other entities and assign them a relative distinguished value such as a distinguished name or, a hash of a certificate. A registration scheme for each registration domain ensures that each registered value is unambiguous within that domain. (*Cf.*, **CERTIFICATION AUTHORITY**)

RELATIVE DISTINGUISHED NAME (RDN)

A set of attributes comprising an entity's distinguished name that distinguishes the entity from others of the same type.

RELY / RELIANCE (ON A CERTIFICATE AND DIGITAL SIGNATURE)

To accept a digital signature and act in a manner that could be detrimental to oneself were the digital signature to be ineffective. (*Cf.*, **RELYING PARTY; RECIPIENT**)

RELYING PARTY

A recipient who acts in reliance on a certificate and digital signature. (*Cf.*, **RECIPIENT; RELY OR RELIANCE (**on a **CERTIFICATE and DIGITAL SIGNATURE)**)

RENEWAL

The process of obtaining a new certificate of the same class and type for the same subject once an existing certificate has expired.

REPOSITORY

A database of certificates and other relevant information accessible on-line.

REPUDIATION (*SEE ALSO* NONREPUDIATION)

The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REVOKE A CERTIFICATE (*SEE ALSO* CERTIFICATE REVOCATION)

The process of permanently ending the operational period of a certificate from a specified time forward.

RSA

A public key cryptographic system invented by Rivest, Shamir & Adelman.

S

SECRET SHARE

A portion of a cryptographic secret split among a number of physical tokens

SECRET SHARE HOLDER

An authorized holder of a physical token containing a secret share.

SECRET SHARE ISSUER

The person designated by an CA to create and distribute secret shares.

SECRET SHARING (*SEE ALSO* SECRET SHARE)

The practice of distributing secret shares of a private key to a number of secret share holders; threshold-based splitting of keys.

SECURE CHANNEL

A cryptographically enhanced communications path that protects messages against perceived security threats.

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations.

SECURITY POLICY

A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system in support of the PCS.

SECURITY SERVICES

Services provided by a set of security frameworks and performed by means of certain security mechanisms. Such services include, but are not limited to, access control, data confidentiality, and data integrity.

SELF-SIGNED PUBLIC KEY

A data structure that is constructed the same as a certificate but that is signed by its subject. Unlike a certificate, a self-signed public key cannot be used in a trustworthy manner to authenticate a public key to other parties. A PCA self-signed public key digitally signed by the VR shall constitute a certificate. (*Cf.,* **CERTIFICATE**)

SERIAL NUMBER (*SEE* CERTIFICATE SERIAL NUMBER)

SERVER

A computer system that responds to requests from client systems.

SIGN

To create a digital signature for a message, or to affix a signature to a document, depending upon the context.

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. (*Cf.,* DIGITAL SIGNATURE)

SIGNER

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

SMART CARD

A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/MIME

A specification for E-mail security exploiting a cryptographic message syntax in an Internet MIME environment.

SOFTWARE PUBLISHER'S PLEDGE

The representations and guarantees made by individual and commercial software publishers as stated in the CPS. (*See* CPS § 4.3)

SOFTWARE VALIDATION

GlobalSign services which provide assurances in accordance with the CPS and the software publisher's pledge (*see* CPS § 4.3) of an individual or commercial software publisher that digitally-signed software was duly published by the subject of the corresponding GlobalSign-issued certificate and has not been undetectably modified since it was digitally signed. (*Cf.,* **INDIVIDUAL SOFTWARE PUBLISHER CERTIFICATE; COMMERCIAL SOFTWARE PUBLISHER CERTIFICATE; SOFTWARE PUBLISHER'S PLEDGE; VALIDATION (OF CERTIFICATE APPLICATION)**)

SUBJECT (OF A CERTIFICATE)

The holder of a private key corresponding to a public key. The term "subject" can refer to both the equipment or device that holds a private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name which is bound to the public key contained in the subject's certificate.

SUBJECT NAME

The unambiguous value in the subject name field of a certificate which is bound to the public key.

SUBSCRIBER

A person who is the subject of, has been issued a certificate, and is capable of using, and authorized to use, the private key that corresponds to the public key listed in the certificate. (*See also* **SUBJECT**; *cf.,* **CERTIFICATE APPLICANT; USER**)

SUBSCRIBER AGREEMENT

The agreement executed between a subscriber and an CA for the provision of designated public certification services in accordance with this CPS.

SUBSCRIBER INFORMATION

Information supplied to a certification authority as part of a certificate application. (*Cf.,* **CERTIFICATE APPLICATION**)

SUSPEND A CERTIFICATE

A temporary "hold" placed on the effectiveness of the operational period of a certificate without permanently revoking the certificate. A certificate suspension is invoked by, *e.g.,* a CRL entry with a reason code. (*Cf.,* **REVOKE A CERTIFICATE**)

T

THREAT

A circumstance or event with the potential to cause harm to a system, including the destruction, unauthorised disclosure, or modification of data and/or denial of service.

TIME STAMP

A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

TOKEN

A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

TRANSACTION

A computer-based transfer of business information which consists of specific processes to facilitate communication over global networks.

TRUST

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and an CA. An authenticating entity must be certain that it can trust the CA to create only valid and reliable certificates, and users of those certificates rely upon the authenticating entity's determination of trust.

TRUSTED PERSON

A person who serves in a trusted position and is qualified to serve in it in accordance with this CPS. (*Cf.*, **TRUST; TRUSTED POSITION; TRUSTED THIRD PARTY; TRUSTWORTHY SYSTEM**)

TRUSTED POSITION

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

TRUSTED THIRD PARTY (TTP)

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship. (*Cf.,* **TRUST**)

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognised in classified government nomenclature.

TYPE (OF CERTIFICATE)

The defining properties of a certificate which limit its intended purpose to a class of applications uniquely associated with that type.

U-V

UNAMBIGUOUS NAME (*SEE* DISTINGUISHED NAME)

UNIVERSAL RESOURCE LOCATOR (URL)

A standardised device for identifying and locating certain records and other resources located on the World Wide Web.

USER

An authorised entity that uses a certificate as applicant, subscriber, recipient or relying party, but not including the CA issuing the certificate. (*Cf.,* **CERTIFICATE APPLICANT; ENTITY; PERSON; SUBSCRIBER**)

VALID CERTIFICATE

A certificate issued by an CA and accepted by the subscriber listed in it.

VALIDATE A CERTIFICATE (*I.E.*, OF AN END-USER SUBSCRIBER CERTIFICATE)

The process performed by a recipient or relying party to confirm that an end-user subscriber certificate is valid and was operational at the date and time a pertinent digital signature was created.

VALIDATE A CERTIFICATE CHAIN

For each certificate in a chain, the process performed by the recipient or relying party to authenticate the public key (in each certificate), confirm that each certificate is valid, was issued within the operational period of the corresponding CA certificate, and that all parties (CAs, end-user subscribers, recipients, and relying parties) have operated in accordance with this CPS as to all certificates in the chain.

VALIDATION (OF CERTIFICATE APPLICATION)

The process performed by the CA (or its LRA) following submission of a certificate application as a prerequisite to approval of the application and the issuance of a certificate. (*Cf.,* **AUTHENTICATION; SOFTWARE VALIDATION**)

VALIDATION (OF SOFTWARE) (*SEE* SOFTWARE VALIDATION)

VERIFY (A DIGITAL SIGNATURE)

In relation to a given digital signature, message, and public key, to determine accurately that (i) the digital signature was created during the operational period of a valid certificate by the private key

corresponding to the public key contained in the certificate and (ii) the associated message has not been altered since the digital signature was created. (*Cf.*, **AUTHENTICATION**; **CONFIRM**)

W-Z

WORLD WIDE WEB (WWW)

A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

WRITING

Information in a record that is accessible and usable for subsequent reference.

X.509

The ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

***

13.2 Index

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W