In support of GlobalSign public PKI services

GlobalSign Certification Practice Statement

Version 4.0
Publication Date: 15 July 2001

Approved by the GlobalSign Policy Board

Contents

Acknowledgments

GlobalSign acknowledges Prof. Jos Dumortier, Katolieke Universiteit Leuven and Otto Vermeulen, PriceWaterhouseCoopers for their comments in this or past versions of the GlobalSign CPS.

GlobalSign acknowledges the work of the:

- Qualified Certificate Policy ETSI TS 101 456 of the Specialist Task Force 155 of the European Telecommunications Standards Institute (ETSI);
- Information Security Committee of the American Bar Association.

1 Introduction

This section gives a brief introduction to the GlobalSign CPS.

This CPS applies to all public services of GlobalSign. This CPS comprises the parts included in the Table of Contents as well as any other documents published through the GlobalSign repository at: http://www.globalsign.net/repository as may be indicated from time to time that may not have been actually integrated in the current published version.

The structure of this CPS addresses the organisational break down of the CA functions addressing technology, organisational aspects, practices and procedures, legal conditions of issuance and a per product presentation of the specific conditions of issuance. In line with EU regulations this CPS also comprises GlobalSign's Privacy, Consumer and Insurance policies to give a granular view of the level of service currently available by GlobalSign.

1.1 Structure

This CPS contains a general part and a specific per-product part. The general part addresses the conditions applicable on all products. The specific part addresses conditions associated with specific GlobalSign products. The following table describes the relationship among the various parts of the GlobalSign CPS:

<table>
<tr><td colspan="3">GlobalSign Certification Practice Statement</td></tr>
<tr><td colspan="3">Parties of GlobalSign PKI services</td></tr>
<tr><td colspan="3">Technology</td></tr>
<tr><td colspan="3">Organisation
Practices and Procedures</td></tr>
<tr><td colspan="3">Legal Conditions</td></tr>
<tr><td colspan="3">Data protection Policy</td></tr>
<tr><td colspan="3">Consumer Policy</td></tr>
<tr><td colspan="3">Insurance Policy</td></tr>
<tr><td colspan="3">Products Policies</td></tr>
<tr><td>Product 1</td><td>Product 2</td><td>Product x</td></tr>
</table>

1.2 Example case of using this CPS

After carefully reading through and approving the subscriber agreement, an applicant for a GlobalSign PersonalSign 2 certificate would refer to section 13 for information on the specific conditions and requirements to issue a GlobalSign PersonalSign 2 certificate. For general conditions on the organisation of GlobalSign the applicant would have to turn to section 5 while to receive information on GlobalSign's insurance scheme it would have to turn to section 10.

1.3 Comments

GlobalSign accepts comments regarding this CPS addressed to: legal@globalsign.net or by post to GlobalSign, attn. Legal Practices, Haachtsesteenweg 1426, B-1130 Brussels, Belgium.

2 General

This section describes the GlobalSign certification services.

2.1 GlobalSign

GlobalSign is a Trust Service Provider and an international network of Trusted Third Parties (TTP's) sharing the GlobalSign procedures and using suitable brand name to issue high quality and highly trusted digital certificates to public and private entities. The main activities of GlobalSign are to:

- Build and manage an international network of CAs and RAs, establishing the brand name of GlobalSign as a universal Trusted Third Party in PKI.
- Provide Managed PKI Services for outsourced PKI projects.
- Provid e Project Management on technology, organisation, procedures and legal aspects of PKI projects.

The GlobalSign public certification services aim at supporting secure electronic commerce and on-line business services to address the business and personal requirements of the users of digital signatures. Through its extended trusted network and diverse PKI products and services, GlobalSign aims at creating a network of Trust in open electronic commerce.

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

2.2 Digital Certificates

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants. Digital certificates are used as a digital equivalent of an identification card.

By means of a digital certificate, GlobalSign provides confirmation of the relationship between a named entity (subscriber) and its public key. The process to obtain a digital certificate includes the identification, naming, authentication and registration of the client as well as the issuance, revocation and expiration of the digital certificate. By means of this procedure to issue digital certificates, GlobalSign provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such entity uses.

2.3 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, GlobalSign may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration.

2.4 Secure Devices and Private Key Protection

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

2.5 Selecting a Certification Service

Although GlobalSign currently offers a range of certificates, it disclaims that its model is entirely tamperproof. To support users in selecting the appropriate PKI service or product GlobalSign offers PKI training on demand, and invites subscribers and partners to study specific requirements of their applications before applying for a GlobalSign certificate.

2.6 Operational Controls

GlobalSign takes certain operational controls including organisational, human resources, and other management-related controls, commensurate with the level of service it offers and the requirements of a partner.

2.7 Gender References

When reference is made to a person in association with a gender, it is implied that reference is made to both genders.

3 Parties of GlobalSign PKI Services

This part refers to the parties involved in the lifecycle of GlobalSign public PKI services.

3.1 GlobalSign Certification Authority

A Certification Authority is an organisation that issues digital certificates. GlobalSign is a Certification Authority. Sometimes, a certification authority is also described by the term issuing authority.

GlobalSign is also responsible to draft the policy prevailing in issuing a certain type or class of digital certificate. GlobalSign is also a Policy Authority while this Certification Practice Statement is a policy for the issuance of GlobalSign digital certificates.

To provide notice or knowledge to relying parties functions associated with the revoked and/or suspended certificates require appropriate publication in a certificate revocation list. GlobalSign operates such a list.

3.2 GlobalSign Certification Authorities and Partners

GlobalSign supports the PKIs of other CAs at pre-defined levels. Within a PKI, such CAs may be of a lower hierarchical position while they retain a service level that is equivalent to that of GlobalSign through appropriate accreditation, auditing and application of procedures. A lower level CA issues certificates on the basis of:

- a technology partnership with GlobalSign;
- GlobalSign provided or audited practices and procedures.

Pursuant to GlobalSign's widely embedded top root certificate and in its function as a root CA and an operator of a network of CAs and RAs, GlobalSign can also perform the root signing of CAs to facilitate interoperability and invoke trust while providing widespread acceptance and trust of the certificates of a third-party CA.

3.3 GlobalSign Registration Authorities and Local Registration Authorities

GlobalSign reaches its subscribers through a network of appropriately selected GlobalSign Registration Authorities (RA) and Local Registration Authorities (LRA). Such parties interact with both the subscriber and GlobalSign to deliver public PKI services to the end-user. GlobalSign RA/LRAs:

- accept, evaluate, approve or reject the registration of certificate applications;
- register subscribers to GlobalSign certification services;
- attend all stages of the identification of subscribers as assigned by GlobalSign according to the type of certificate they issue;
- use official, notarised or otherwise indicated document to evaluate a subscriber application;

- following approval of an application notifies GlobalSign to issue a certificate;
- initiate the process to revoke a certificate and request a certificate revocation from GlobalSign.

GlobalSign RA/LRAs act locally within their own context of geographical or business partnerships on approval and authorisation by GlobalSign. GlobalSign RA/LRAs act in accordance with GlobalSign's practices and procedures. There is no limitation to the number of RAs that may be associated with GlobalSign. GlobalSign provides RA/LRAs with the necessary technology and know-how to obtain a high level of training in accordance with GlobalSign accreditation requirements.

A LRA performs registration tasks on behalf of a RA. A RA supervises an LRA. A LRA may have a geographical or business connotation and it operates within the framework of GlobalSign's own or GlobalSign accredited procedures. A RA may support several LRAs.

3.4 Subscribers

Subscribers of GlobalSign services are entities including natural persons (individuals) and/or legal persons (companies) that use PKI services. Subscribers are parties that:

- apply for a certificate;
- are identified in a certificate
- hold the private key corresponding to the public key that is listed in a subscriber certificate.

3.5 Relying Parties

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

To verify the validity of a digital certificate they receive, relying parties must always refer to the GlobalSign Certificate Revocation List (CRL) prior to relying on information featured in a certificate.

4 Technology

This section addresses certain technology aspects of the GlobalSign infrastructure and PKI services.

4.1 Digital Certificate Management

GlobalSign certificate management, at large, refers to functions that include the following:

- identification of a certificate applicant;
- authorisation of the issuance of certificates;
- issuance of certificates;
- revocation of certificates;
- eventual storing of a certificate on a portable medium;
- de-commissioning of the corresponding private keys through a process involving the revocation of certificates;
- listing certificates;
- distributing certificates;
- publishing certificates;
- storing certificates;
- retrieving certificates in accordance with their particular intended use.

Within the GlobalSign Trust network, overall certification management is a role performed by GlobalSign.

4.2 Types of GlobalSign Certificates

GlobalSign currently offers an array of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications.

GlobalSign may update or extend its list of products, including the types of certificates it issues, as it sees fit. Issued, suspended or revoked certificates are appropriately published on directories. Types of certificates are discussed below in this CPS.

4.3 Extensions and Naming

4.3.1 Standards

To construct digital certificates for its public PKI products and services GlobalSign uses standards that include:

- X.509, version 3;
- specifications of IETF/PKIX RFC 2459;
- WAP Forum/WTLS.

4.3.2 Digital Certificate Extensions

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

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

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

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

4.3.3 Critical Extensions

GlobalSign uses certain critical extension in the certificates it issues such as:

- A basic constraint in the key usage to show whether a certificate is meant for a CA or not;
- to show the intended usage of the key;
- to show the number of levels in the hierarchy under a CA certificate.

4.3.4 Incorporation by Reference

The GlobalSign CPS as well as applicable statements, disclaimers etc. are incorporated in a subscriber's certificate in ways other than full text inclusion as the limitation to 64 bytes of the applicable organisational field in a certificate does not allow for full text inclusion. Documents incorporated by reference contain a statement on it.

GlobalSign reserves its right to limit certain statements including applications for which a certificate may be used, types of users, reliance limits for subscribers and relying parties etc. GlobalSign may further link certain application-specific extensions, as appropriate to disclose relevant policies or CPS sections to the extent that verifying software supports such application.

Extensions and enhanced naming are usually expressed in a subscriber certificate. They can also be partially defined in a subscriber certificate while the remainder can be a shelved document that is incorporated by reference in the subscriber certificate. Information included in such a shelved document can be made available to requesting parties.

Information contained in the organisational unit field is also included in the Certificate Policy extension that GlobalSign may use.

4.3.5 Certificate Policy

GlobalSign may use a Certificate Policy with its subscriber certificate, as it sees appropriate, according to the business or legal context of the application or as it may be mandated for certain products. This CPS is a certificate policy.

GlobalSign acknowledges the Qualified Certificate Policy ETSI TS 101 456 of the Specialist Task Force 155 of the European Telecommunications Standards Institute (ETSI).

4.3.6 Object Identifiers

As a Certificate Policy Authority, GlobalSign may assign to this CPS or any other GlobalSign Certificate Policy an object identifier (OID) that is also included in the certificate policy extension. GlobalSign also uses policy qualifiers that include pointer values, warnings, liability limitations, and warranty disclaimers as described below:

- Pointers are machine or human readable formats that indicate to certificate users the location and access of the CPS and other information.
- Subscriber certificates may include a statement on limitations of liability and disclaimers of warranty. Such a statement may be displayed as a URL or displayed to users upon registration.
- GlobalSign communicates information to users through an enhanced naming organisational unit attribute, a GlobalSign standard qualifier to a GlobalSign certificate policy and other vendor or industry extensions as might be applicable in specific formats.

4.4 GlobalSign Directories and Repository

GlobalSign makes publicly available and manages directories of issued, suspended and revoked certificates to validate the level of Trust in its services. GlobalSign updates frequently its Certificate Revocation List (CRL). GlobalSign also publishes repositories of legal notices regarding its public PKI services, including this CPS as well as any other information it considers essential to its services. Checking and validating the status of Trust of issued and revoked certificates is a task for users and relying parties.

GlobalSign updates its CRLs in three-hour intervals.

4.4.1 Standards used for GlobalSign Directories

To construct schemes for its public directories, GlobalSign uses standards that include:

- IETF/PKIX RFC 2459;
- IETF/PKIX OCSP RFC 2560;
- IETF/PKIX LDAP version 2, Schema RFC 2587.

4.5 Standards Used for GlobalSign Certificate Requests

To construct certificate requests GlobalSign uses standards that include:

- PKCS#10
- Microsoft IE
- Netscape certificate request

- Nokia/WTLS.

4.6 Subscriber Identification

Prior to issuing a certificate GlobalSign may mandate controls to establish the identity of a subscriber. Such controls are the role of a GlobalSign RA or LRA that also supervises such procedures on the basis of GlobalSign issued guidelines that are to be used on-line and/or off-line.

4.7 Software and Hardware Devices

GlobalSign accredits all hardware and software it uses for its public PKI and uses only third party accredited and trustworthy equipment for key generation, user authentication, certificate registration, audit and archival. GlobalSign discloses such information to selected parties as it may be required or mandated by the circumstances.

4.8 GlobalSign Private Key Generation Process

GlobalSign uses a trustworthy process for the generation of its root private key according to a documented procedure. GlobalSign distributes the secret shares of its private key(s). GlobalSign is the owner of the private key(s) and has the authority to transfer such secret shares to authorised secret-shareholders.

4.8.1 GlobalSign Private Key Usage

The private key of GlobalSign is used to sign GlobalSign issued certificates, GlobalSign certification revocation lists and accredited root-signed entities.

4.8.2 GlobalSign Private Key Type

GlobalSign makes use of the MD5/RSA algorithm with a key length of 2048 bits and a validity period of 15 years.

4.8.3 GlobalSign Key Generation

GlobalSign securely generates and protects its own private key(s), using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of it. GlobalSign implements and documents key generation procedures, in line with this CPS. GlobalSign acknowledges public, international and European standards on trustworthy systems.

4.8.4 GlobalSign Key Generation Devices

The generation of the private key of GlobalSign occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirements.

4.8.5 GlobalSign Key Generation Controls

The generation of the private key of GlobalSign requires the control of more than one appropriately authorised members of staff serving in trustworthy positions. More than one members of the management make authorisation of key generation in writing.

4.9 GlobalSign Private Key Storage

GlobalSign uses a secure cryptographic device to store its own private key meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirements.

4.9.1 GlobalSign Key Storage Controls

The storage of the private key of GlobalSign requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. More than one members of the management make authorisation of key storage and assigned personnel in writing.

4.9.2 GlobalSign Key Back Up

GlobalSign's private key is backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. More than one members of the management make authorisation of key storage and assigned personnel in writing.

4.9.3 Secret Sharing

GlobalSign secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of private key(s) and provide for key recovery.

4.9.4 Acceptance of Secret Shares

Before secret shareholders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody.

A secret shareholder receives the secret share within a physical medium, such as a GlobalSign approved hardware cryptographic module. GlobalSign keeps written records of secret share distribution.

5 Organisation

This part describes the Organisation and the Trust conditions of the provision of public GlobalSign services.

5.1 GlobalSign Infrastructure

As a root CA and a Trust service provider, GlobalSign strives to maintain its:

- sound organisation;
- advanced technology;
- Trust network;
- framework of published and/or audited practices and procedures according to which it operates.

5.2 Organisational Good Standing

GlobalSign makes reasonable efforts to be in good standing with (and, where applicable, accredited, certified, or licensed by) applicable organisations and authorities whose rules and regulations might materially affect GlobalSign's trustworthiness and as required by law or contract.

GlobalSign is an organisation that is frequently audited for its financial stability.

5.3 Business Continuity

GlobalSign has a business continuity plan to restore business operations in a reasonably timely manner following interruption to, or failure of critical business processes.

5.4 Conformance to this CPS

GlobalSign conforms to this CPS and obligations found in adjacent contracts.

5.5 Trustworthy Systems

In performing its services, GlobalSign makes use of trustworthy and appropriately accredited systems.

5.6 Termination of CA Operations

Before terminating its CA activities, GlobalSign:

- Provides subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revokes all certificates that are still unrevoked or unexpired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Gives timely notice of revocation to each affected subscriber.
- Makes reasonable arrangements to preserve its records according to this CPS.

- If possible, it provides succession arrangements for the re-issuance of Certificates by a successor CA under the same CPS.

GlobalSign may update this clause, as it might be necessary.

5.7 Accreditation of Entities

GlobalSign accredits all entities that enter or operate within its own PKI hierarchy, including CAs, RAs, and LRAs, individual employees in trusted positions. Accreditation may be effected by a self-declaration or agreement.

5.8 GlobalSign Accreditation

GlobalSign takes steps to comply with CA accreditation schemes, as they become available.

5.9 Financial Resources

GlobalSign has sufficient financial resources to maintain operations and perform duties. GlobalSign is reasonably able to bear the risk of liability to subscribers and recipients of certificates as well as any other parties that may rely on information included in the certificates issued.

5.10 Insurance

GlobalSign makes available a limited warranty insurance policy for selected types of its products or services to cover against commonly identified risks of digital certification.

5.11 Compliance Documentation

GlobalSign keeps records in a trustworthy manner. Such documentation supports:

- Compliance with this CPS.
- Audit reports by external parties.
- Audit reports as made available by relevant accreditation schemes.
- Information in support of each digital certificate it issues and especially with regard to the creation, issuance, use, suspension, revocation, expiration, and renewal or re-enrolment.

5.12 Form of Records

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

5.13 Records Retention

GlobalSign retains in a trustworthy manner records of GlobalSign digital certificates for a term as follows:

- PersonalSign 1™ certificates or equivalent for no less than one (1) year;
- PersonalSign 2™ certificates, GlobalSign Secure Server, GlobalSign Object Publishing, GlobalSign HyperSign 128 or equivalent for no less than five (5) years;
- PersonalSign 3™ certificates, for no less than 30 years.
- For public certificates, based on accreditation schemes as prescribed on such scheme.

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

GlobalSign may revise record retention terms as might be required to comply with accreditation schemes.

5.14 Logs for Core Functions

GlobalSign maintains in a trustworthy manner logs of the following events:

- key generation;
- key management;
- interruption of service;
- perimeter controls.

5.14.1 Accessing Logs for Core Functions

Accessing logs for core function is restricted to authorised CA and RA administrators and personnel while GlobalSign may allow accessing of external parties as it may be required by the circumstances.

5.14.2 Protection of Logs for Core Functions

GlobalSign employs dual control to protect the integrity of logs for core functions.

5.15 Audit for Core Functions

GlobalSign seeks auditing through specialised auditors for selected operations and support as it sees fit or as mandated by accreditation schemes. GlobalSign is not obliged to comply with any of the content of such auditing reports and it may review such auditing reports with a view to protect GlobalSign services.

5.16 Availability of GlobalSign Certificates

To verify a signature that is verifiable with reference to a digital certificate GlobalSign may make available to parties copies of certificates in which GlobalSign is the subject as well as any related revocation data.

5.17 Publication

GlobalSign publishes information in its Repository, the CRL and the GlobalSign web site. Updates are denoted as appropriate.

5.17.1 Publication of Information on Issued Certificates

GlobalSign publishes all issued public digital certificates, any revocation data or expiration data on such certificates as well as this CPS on dedicated directories and the GlobalSign Repository.

5.17.2 Accessing Information Published

Accessing information published in the publicly accessible directories and the web site is allowed to all entities.

Proprietary, confidential or otherwise protected information is allowed upon request. GlobalSign shall use its discretion to disclose such information.

5.18 Confidentiality Information

GlobalSign observes personal data privacy rules as explained hereunder. GlobalSign also treats in a confidential manner and as prescribed by law:

- subscriber agreements;
- certificate application records;
- transaction records;
- external or internal auditing trail records and reports;
- contingency plans and disaster recovery plans;
- internal tracks and records on the operations of GlobalSign infrastructure, certificate management and enrolment services and data.

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

- the party to whom GlobalSign owes a duty to keep information confidential the party requesting such information;
- a court order.

GlobalSign may charge an administrative fee to process such disclosures.

5.19 Secure Facilities

GlobalSign operates secure facilities as prescribed in this CPS and according to a documented procedure.

5.19.1 Physical and Environmental Controls

Physical access to the secure part of GlobalSign facilities is limited to appropriately authorised individuals. Certificate issuance facilities are protected from environmental hazards. Loss, damage or compromise of assets and interruption to business activities are detected, and reasonably prevented. GlobalSign takes reasonable steps to prevent against and detect any compromise or theft of information.

5.20 Contingency Plans and Disaster Recovery

GlobalSign systems feature a very high level of availability and redundancy. To maintain the integrity of its services GlobalSign implements, documents, and periodically tests appropriate contingency and disaster recovery plans. GlobalSign discloses such plans to parties as it sees fit or mandated by the circumstances.

5.21 Personnel Management and Practices

GlobalSign follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties according to a documented procedure.

5.21.1 Trusted Positions

GlobalSign personnel includes all employees, co ntractors, and consultants of GlobalSign. All GlobalSign personnel with access to or control over operations (including cryptographic operations) that may materially affect the registration, issuance, usage, suspension, or revocation of certificates, including access to restricted operations of the GlobalSign repository for purposes of this CPS are 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 supervise the GlobalSign infrastructure.

5.21.2 Investigation and Compliance

GlobalSign conducts 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 requires all employees serving in trusted positions to submit an official document attesting that they are of good character and have no prior convictions for serious crimes or file to GlobalSign a declaration of good conduct. GlobalSign conducts periodic investigations of trusted personnel to verify the trustworthiness and competence in accordance with GlobalSign personnel practices.

5.21.3 Confidential Information

All personnel in trusted positions handle all information in strict confidence. All RA and LRA personnel as well as personnel that handles personal data comply with the requirements of the European Directive on the protection of personal data and/or the GlobalSign Privacy Policy.

5.21.4 Task Description

Trusted personnel have clearly defined roles and a job description for their function. Where appropriate, dual control and separation of duties are exercised.

5.21.5 Senior Personnel

Management and senior personnel possess the necessary experience and familiarity with PKI.

5.21.6 Conflicting Interests

No GlobalSign personnel have any conflicting roles or interests with GlobalSign.

5.21.7 Removal and Replacement of Personnel in Trusted Positions

All personnel serving in trusted position who fail an initial or periodic investigation are removed from a trusted position. The removal of any person serving in a trusted position remains exclusively at the sole discretion of GlobalSign.

5.22 Publication of Information

The GlobalSign certificate services and the GlobalSign repository are accessible through several means of communication:

- on the Web from, http://www.globalsign.net/repository/index.cfm
- by e-mail, support@globalsign.net, legal@globalsign.net
- by post, GlobalSign NV, Support, Haachtsesteenweg 1426, B-1130 Brussels, Belgium.

6 Practices and Procedures

This part presents the general aspects of practices and procedures of the GlobalSign Public PKI services. For specific per product information the reader may refer to the dedicated per product section hereunder.

6.1 Certificate Application Requirements for Subscribers

Certificate applicants (collectively called subscribers) must take the following steps prior to requesting a GlobalSign certificate:

- generate a key pair and demonstrate to GlobalSign that it is such a key pair and that the private key corresponds to it;
- protect the integrity of the private key of the generated key pair;
- submit a filled out certificate application;
- agree with the terms of a subscriber agreement and this CPS;
- submit the public key of the generated key pair to GlobalSign;
- provide proof of their identity according to GlobalSign or other standard defined procedures as they may have been acknowledged by GlobalSign.

6.1.1 Delegation

Depending on the type of certificate, an application for a GlobalSign digital certificate can be made in person or through an agent.

6.1.2 Key Pair Generation

Subscribers are exclusively responsible to generate securely their own private key pair, using a trustworthy system as required by the product or application.

6.1.3 Key Pair Protection

Subscribers are exclusively responsible to take all necessary measures to prevent the compromise, loss, disclosure, modification, theft, or otherwise unauthorised use of their private key.

6.1.4 Use of Secure Devices and Products

Unless otherwise stated in this CPS, subscribers (and not GlobalSign) use secure devices and products that provide for the protection of their keys.

6.1.5 Delegating Responsibilities for Private Keys

Subscribers are exclusively responsible for the acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys.

6.2 Validation Information for Certificate Applications

Applications for GlobalSign certificates are supported by appropriate documentation to establish the identity of an applicant as described in the product information below in this CPS.

GlobalSign may modify the requirements related to application information for individuals to respond to own GlobalSign requirements, the business context of the usage of a digital certificate, or as it may be prescribed by law. Such documentation includes identification elements such as the following.

6.2.1 Application Information for Individuals

Critical information elements for a GlobalSign personal certificate may include the following elements. This statement does not create an obligation on the part of GlobalSign to modify its requirements as its sees appropriate, in the business context of the certificate, or as it may be prescribed by law.

- Applicant's e-mail address;
- Legal name
- Country
- Applicant's public key
- Identification data
- Challenge phrase or password
- Payment information
- Subscriber agreement and registration form acknowledged by an RA/LRA pursuant to applicant producing an official form of identification as required.
- Proof of professional context (where applicable).

6.2.2 Application Information for Legal Persons

Critical information elements for a GlobalSign certificate issued to a legal person may include any of the following elements:

- Domain name
- IP address
- Legal Name of the Organisation
- Organisational unit
- 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
- Proof of existence of the Organisation
- Proof of organisational status such as articles of incorporation of a company, letter from office of Dean or Principal (for Educational Institutions), official letter from an authorised representative of a government organisation.
- Registration form signed and properly filled in
- Signed subscriber agreement

5.1 Requirements to Validate Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, GlobalSign confirms the following information:

- the certificate applicant is the same person as the person identified in the certificate request;
- the certificate applicant holds the private key corresponding to the public key to be included in the certificate;
- the information to be published in the certificate is accurate, except for non-verified subscriber information;

- any agents who apply for a certificate listing the certificate applicant's public key are duly authorised to do so.

GlobalSign controls the accuracy of the information published as submitted by the applicant at the moment the certificate is issued.

In all cases and for all types of GlobalSign certificates the subscriber has an obligation to monitor the accuracy of the submitted information and notify GlobalSign of any such changes.

5.1.1 Personal Presence

To establish the link between an applicant and an applicant's public key, GlobalSign may require the personal presence of an applicant before a RA/LRA for certain types or classes of digital certificates while it reserves its right to modify such registration requirements as it sees appropriate or it may be prescribed by law.

5.1.2 Third-Party Confirmation of Business Entity Information

GlobalSign may request third parties to confirm information on a business entity that applies for a GlobalSign digital certificate. GlobalSign accepts confirmation from parties such as chambers of commerce, other third-party databases and government entities while it may examine other third party referees as it may be provided within a certain business context.

Certain entities such as banks and financial institutions may be required to provide proof of their activity prior to having digital certificates issued to them with a purpose to perform banking or otherwise licensed or controlled functions.

GlobalSign may use any means of communication at its disposal to ascertain the identity of a legal entity.

5.1.3 Domain Name Confirmation and Serial Number Assignment

GlobalSign has exclusive discretion to assign Relative Distinguished Names (RDNs) and certificate serial numbers that appear in GlobalSign certificates. GlobalSign may use the Domain Name Service for resolving RDN assignment if necessary.

6.3 Time to Confirm Submitted Data

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

6.4 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application, GlobalSign approves an application for a digital certificate.

If the validation of a certificate application fails, GlobalSign rejects the certificate application. Upon such rejection GlobalSign promptly notifies the

applicant by any means of communication it sees appropriate and provides a reason for such failure to the extent permitted by law.

GlobalSign may reject applications for certificates if on its own assessment, by issuing a certificate to such parties, the good and trusted name of GlobalSign might get tarnished, diminished or have its value reduced. GlobalSign reserves its right to reject applications to issue a certificate to applicants, as it might see fit, without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently reapply.

6.5 Certificate Issuance and Subscriber Consent

GlobalSign issues certificates upon approval of a certificate application. A digital certificate is deemed to be valid upon subscriber's acceptance.

6.6 GlobalSign Representations Upon Certificate Issuance

GlobalSign makes certain representations to subscribers and relying parties as described in the articles below.

6.6.1 GlobalSign Representations to Subscriber

Upon issuance, GlobalSign represents to the subscribers the following:

- a certificate contains no misrepresentations of fact in the certificate known to GlobalSign or originating from GlobalSign;
- there are no transcription errors of data received by GlobalSign originating from the certificate applicant as a result of failure of GlobalSign to exercise reasonable care in creating the certificate;
- the certificate meets all material requirements and issuance conditions as prescribed by this CPS;
- GlobalSign promptly revokes or suspends certificates in accordance with this CPS;
- GlobalSign notifies subscribers of facts known to it that materially affect the validity and reliability of the certificate it issued to such subscriber;
- GlobalSign's private key has not been compromised in any way.

GlobalSign reserves its right to alter such issuance conditions and representations while such changes effect no other obligation to GlobalSign than those foreseen in the GlobalSign Insurance policy below in this CPS.

6.6.2 GlobalSign's Representations to Relying Parties

Upon issuance GlobalSign represents to parties relying on information featured upon a certificate (relying parties) the following:

- the accuracy of information in or incorporated by reference within the certificate at the time of issuance of a certificate, except for non verified subscriber information;
- GlobalSign has complied with this CPS when issuing a digital certificate;
- at the time of issuance GlobalSign's private key had not been compromised in any way.

GlobalSign reserves its right to require relying parties to act according to certain conditions of usage when accessing the public information repository and its web site as described b elow in this CPS. GlobalSign also extends to relying parties a conditional insurance program for certain types of damages as described below in this CPS.

6.6.3 GlobalSign Representations Upon Publication

By publishing a certificate, GlobalSign represents that it has issued the certificate to the subscriber and that the subscriber has accepted the certificate.

6.7 Certificate Validity

Certificates are valid upon issuance by GlobalSign and acceptance by the subscriber.

6.8 Certificate Acceptance by Subscribers

A subscriber is deemed to have accepted a certificate when approval is manifested through means such as those described below:

- On-line: Via a secure WWW link (https). The subscriber must notify GlobalSign of any inaccuracy or defect in a certificate immediately after receipt of the certificate or earlier notice of any content that is to be included in the certificate.
- E-mail (S/MIME): Upon completion of a validation procedure GlobalSign sends the certificate to the e-mail address of the applicant. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of any content that is to be included in the certificate.

If no notification of acceptance is received a certificate is deemed accepted on the moment the payment becomes final or the subscriber first uses the certificate, whatever occurs first.

6.8.1 Representations by Subscriber Upon Acceptance

Upon accepting a certificate the subscriber represents to GlobalSign and to relying parties that at the time of acceptance:

- Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.
- All representations made by the subscriber to GlobalSign regarding the information contained in the certificate are accurate and true.
- All information contained in the certificate is accurate and true to the best of the subscriber's knowledge or to the extent that the subscriber had notice of such information.
- The subscriber promptly notifies GlobalSign of any material inaccuracies in submitted information.

- The certificate is used exclusively for authorised and legal purposes, consistent with this CPS.
- Use a GlobalSign certificate only in conjunction with the entity named in the organisation field of a digital certificate (if applicable).
- The subscriber retains control of its private key, use a trustworthy system, and take reasonable precautions to prevent its loss, disclosure, theft, modification, or unauthorised use.
- 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.
- The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of GlobalSign.
- The subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The subscriber complies with all export laws and regulations for dual usage goods as may be applicable.
- The subscriber follows applicable standards in the application.
- The subscriber does not use the same public key to obtain another digital certificate for the same identity name requested.

6.9 Publication of Issued Certificates

Upon subscriber's acceptance of the certificate, and checking by GlobalSign, GlobalSign publishes a copy of the certificate in a GlobalSign repository and/or in any other repositories, as GlobalSign may determine it. Subscribers on may also publish their GlobalSign certificates in repositories.

6.10 Verification of Digital Signatures

Verification of a digital signature aims at determining that:

- the digital signature has been created by the private key corresponding to the public key listed in the signer's certificate;
- the associated message has not been altered since the digital signature was created.

To verify a digital signature a user must take steps such as those described in the clauses below:

- *Establish a certificate chain* : A digital signature is verified through confirmation of a certificate chain. In case of cross certification, multiple certificate chains may lead from a root to a certificate. In such case the verifier may have multiple options to select and validate a certificate chain.
- *Check revocation/suspension of a certificate*: The recipient of a certificate must check any revocations or suspension of a certificate against a published CRL that GlobalSign makes available in its Repository.

- *Delimiting signed data*: To verify a digital signature it is necessary to know precisely what data has been signed. A standard signed message format may be specified to accurately denote the signed data.
- *Time-stamping*: Time stamping can be used to determine the time and date on which a digital signature is affixed.
- *Signature policy*: Statements such as a signature policy may be used to establish the scope of a digital signature or address specific requirements like the European Qualified Certificates. In certain signing environments such as in EDI, digital signatures are classified as specified security services with defined semantics. GlobalSign supports signature policies to define the operational background and context of usage of a digital signature.
- *End-user subscriber private key*: For specific applications, GlobalSign may limit the purposes for which a private key corresponding to the public key included in a certificate it issues may be used.
- *Confirmation of a certificate chain*: Confirmation of a certificate chain is the process of validating a certificate chain and subsequently validating an end-user subscriber certificate.

6.11 Effect of Validating a Subscriber Certificate

A digital signature can be binding against the signer if:

- It is so prescribed by law.
- It was created within the operational period of a digital certificate.
- It can be properly verified by confirmation of a certificate chain.
- A relying party has no knowledge or notice of a breach of the requirements of this CPS by the signer.
- The relying party has complied with all requirements of this CPS.

Relying on unverified digital signature is undertaken on the relying party's own risk. GlobalSign has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository.

6.12 Reliance on Digital Signatures

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the verifier. A digital signature can be trusted to rely upon if:

- The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate;
- Reliance is reasonable under the circumstances.

6.13 Certificate Suspension and Revocation

Upon request from a GlobalSign RA, GlobalSign suspends or revokes a digital certificate 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 has breached a material obligation under this CPS.
- The performance of a person's obligations under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.

A subscriber contacts a GlobalSign RA to request suspension or revocation. GlobalSign suspends or revokes a certificate promptly upon verifying the identity of the requesting party and confirming that it has not been issued in accordance with the procedures required by this CPS. Verification of the identity can be done through information elements featured in the identification data the subscriber has submitted to the GlobalSign RA.

6.13.1 Term and Termination of Suspension and Revocation

Suspension may last for as long as it is required to establish the conditions that caused the request of suspension. Following negative proof of such conditions a subscriber may request the re-activation of a certificate.

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

During suspension, or upon revocation of a certificate, the operational period of that certificate is immediately considered terminated.

To keep intact the capacity of users of digital certificates to digitally sign, approximately thirty (30) days prior expiration of a digital certificate, GlobalSign makes reasonable efforts to notify subscribers via e-mail, of the imminent expiration of a digital certificate.

6.14 Renewal

Requirements for renewal of a digital certificate may become available and vary from these originally required for subscribing to the service.

7 Legal Conditions of Issuance

This part describes the legal representations, warranties and limitations associated with the provision of GlobalSign public PKI services.

7.1 Representations of GlobalSign

GlobalSign makes to all subscribers and relying parties certain representations regarding its public services, as described below. GlobalSign reserves its right to modify such representations as it sees fit or required by law.

7.2 Public Services Only

This CPS applies to all public services of GlobalSign as featured on the public web site of GlobalSign.

7.3 Information Incorporated by Reference in a Digital Certificate

GlobalSign incorporates by reference the following information in digital certificates it issues:

- terms and conditions in this CPS;
- any other applicable certificate policy as may be stated on an issued GlobalSign certificate;
- the mandatory elements of applicable standards;
- any non-mandatory but customised elements of applicable standards;
- content of extensions and enhanced naming not addressed elsewhere;
- any other information that is indicated to be so in a field of a certificate.

7.4 Pointers to Incorporate by Reference

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

7.5 CPS Revision Procedure

GlobalSign may make revisions and updates to this CPS according to a documented internal procedure, major elements of which can be found below.

7.5.1 Versions

Versions are indicated by a number code composed by an integer and a decimal number. Minor changes are indicated by a change of the decimal number. A publication date is also indicated.

7.5.2 GlobalSign Policy Board

The GlobalSign Policy Board must approve new versions and published updates of the GlobalSign CPS. All members of the GlobalSign Policy Board may vote.

7.6 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the GlobalSign CPS Board such CPS is published in the GlobalSign online Repository at http://www.globalsign.net/repository.

GlobalSign publishes a notice of such updates on its public web site at http://www.globalsign.net and provides notice to subscribers of such updates.

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

7.7 Displaying Liability Limitations, and Warranty Disclaimers

GlobalSign certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period and intended purpose of the certificate and disclaimers of warranty that may apply. Such information may alternatively be displayed through a hypertext link.

7.8 Publication of Certificate Data

GlobalSign reserves its right to publish a certificate and certificate related data in its CRL or any other accessible repositories as indicated.

As GlobalSign manages directories of featured certificates to enhance the level of Trust in its services users and relying parties are strongly advised to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a certificate.

7.9 Monitoring the Accuracy of Submitted Information

In all cases and for all types of GlobalSign certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify GlobalSign of any such changes.

7.10 Interference with a GlobalSign Implementation

Subscribers, relying parties and any other parties refrain from monitoring, interfering with, or reverse engineering the technical implementation of GlobalSign PKI services including the key generation process, the public web site and the GlobalSign repositories except as explicitly permitted by this CPS or upon prior written approval of GlobalSign.

7.11 Compliance with Software Standards

User software must be compliant with applicable standards and enforces the requirements set out in this CPS. GlobalSign does not warrant that user software supports and enforces controls required by GlobalSign while the user should seek appropriate advice.

7.12 Root Signing Partnerships

7.12.1 GlobalSign Root Sign Partnership Limitations

Partners of the GlobalSign network including RAs and LRAs refrain from undertaking any actions that might imperil, put in doubt or reduce the trust associated with the GlobalSign products and services. GlobalSign partners specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities without GlobalSign's written permit.

7.12.2 GlobalSign Limitation of Liability for a GlobalSign Partner

As the GlobalSign network may include partners, including CAs, RAs etc. that operate under GlobalSign practices and procedures, GlobalSign warrants the integrity of certificates issued under its own root within the limits of the GlobalSign insurance policy featured below in this CPS.

GlobalSign disclaims any and all liability associated with the integrity or the functionality of any service or product made available by such partner to the extent that such service or product is not covered by the GlobalSign insurance policy featured below in this CPS. The liability for such service or product remains exclusively with the partner making such service or product available i.e. the GlobalSign partner and not with GlobalSign.

7.12.3 Root Sign Limitation of Liability

As the GlobalSign network may include CAs that have been root signed by GlobalSign, GlobalSign offers limited warranty of the integrity of such link between its own root and the root of a root signed CA.

GlobalSign disclaims any and all liability associated with the integrity or the functionality of any subscriber certificate issued under such partner root. The liability for such link remains exclusively with the issuer of such certificate i.e. the GlobalSign partner and not with GlobalSign.

7.13 Renewal

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

7.14 Secret Shares

GlobalSign uses secret shares to protect its private key.

7.14.1 Safeguarding Secret Shares

7.14.1.1 Safeguarding Secret Shares by a secret shareholder

The secret shareholder of a cryptographic module uses a trustworthy system to protect the secret share against compromise as prescribed by GlobalSign procedures and provided by GlobalSign. Except, as provided in this CPS, the secret shareholder will not:

- Disclose, copy, make available to third parties, or make any unauthorised usage whatsoever of such secret share.
- Reveal (expressly or implicitly) that the shareholder, or any other secret shareholder, is a secret shareholder.
- Store the secret share in a location that fails to provide for its recovery in the event the secret shareholder becomes incapacitated or unavailable (except when the secret share is being used for authorised purposes).

7.14.1.2 Safeguarding Secret Shares by GlobalSign

GlobalSign takes all steps necessary to store its secret shares in a secure environment with a view to safeguard their integrity at all times.

7.14.2 Record Keeping by Secret Share Issuers and Holders

Secret share issuers and holders keep records of activities pertaining to all secret share materials. The secret shareholder provides information on the status of the secret share to the secret share issuer upon request.

7.14.3 Secret Shareholder Liability

The secret shareholder performs all associated obligations under this CPS and must act in a reasonable and careful manner. The secret shareholder notifies the secret share issuer of any loss, theft, improper disclosure, or compromise of the secret share immediately upon taking notice of it. The secret shareholder is not responsible for failure to fulfil any obligations due to causes beyond its reasonable control. The secret shareholder is liable for improper disclosure of secret shares or failure to notify the secret share issuer of improper disclosure or compromise through its fault, including negligence or recklessness.

7.14.4 Indemnity by Secret Share Issuer

The secret share issuer agrees to indemnify and hold harmless the secret share holder from all claims, actions, damages, judgments, 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 gross negligence or error.

7.15 Choice of Cryptographic Methods

Parties acknowledge that they are solely responsible for choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

7.16 Reliance on Non Verified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all time by checking the validity of a digital certificate against a CRL or any other available directory published by GlobalSign as an unverified digital signature cannot be assigned as the signature of a subscriber.

Relying on a non-verifiable digital signature may result to risks that the relying party and not GlobalSign assume in whole.

7.17 Refusal to Issue a Certificate

GlobalSign may use its own discretion and refuse to issue a certificate to any party.

7.18 Public Keys of Refused Applications

Applicants for certificates that have not resulted in an successfully issued GlobalSign certificate for any reason whatsoever may never use the submitted public key included in a certificate corresponding to a private key public key if the effect is to create the conditions of relying upon such a certificate.

7.19 Subscriber Obligations

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

- Having knowledge and if necessary seek training on using digital certificates and PKI.
- To generating securely their private key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with GlobalSign.
- Ensure that the public key submitted to GlobalSign corresponds to the private key used.
- Ensure that the public key submitted to GlobalSign is the correct one.
- Generating a new, secure key pair to be used in association with a certificate that they request from GlobalSign.
- Reading, understanding and agreeing with all terms and conditions in this GlobalSign CPS and associated policies published in the GlobalSign Repository.
- Refraining from tampering with a GlobalSign certificate.
- Using GlobalSign certificates for legal and authorised purposes in accordance with this GlobalSign CPS.
- Notifying GlobalSign or a GlobalSign RA of any changes in the information submitted.
- Ceasing using a GlobalSign certificate if any featured information becomes invalid.
- Ceasing using a GlobalSign certificate when it becomes invalid.
- When invalid, remove server certificates from any applications and/or devices they have been installed on.
- Using only one certificate at a given time.

- Refraining from using the subscriber's private key corresponding to the public key in a GlobalSign issued certificate under its name to have other certificates issued.
- Using a GlobalSign certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- Using secure devices and products that provide appropriate protection to their keys.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting to GlobalSign or any GlobalSign directory any material that contains statements that violate any law or the rights of any party.
- Request the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a GlobalSign certificate.
- Appropriately supervise agents or partners that apply for or use a GlobalSign certificate on behalf of the subscriber.
- Controlling the data agents submit to GlobalSign and notify GlobalSign of any misrepresentation and omission made by an agent.

7.20 Indemnity

The subscriber agrees to indemnify and hold GlobalSign 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 may incur as a result of:

- **Any false or misrepresented data supplied by the subscriber or its agent(s).**
- **Any failure of 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.**
- **Failure to protect the subscriber's private key, to use a trustworthy system as required, or to take precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key or to attnd to the integrity of the GlobalSign Root.**
- **Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.**

7.21 Relying Party Obligations

A party relying on a GlobalSign certificate promises to:

- Have knowledge on using digital certificates and PKI.
- Receive notice of the GlobalSign CPS and associated conditions for relying parties.

- Verify a GlobalSign certificate by using among others a CRL (including the GlobalSign CRL) in accordance with the certificate path validation procedure.
- Trust a GlobalSign certificate only if all information featured on such certificate can be verified as being correct and updated.
- Rely on a GlobalSign certificate, as it may be reasonable under the circumstances.

7.22 Subscriber Liability Towards Relying Parties

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

7.23 GlobalSign Repository and Web site Conditions

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

- Information provided as a result of the search for a digital certificate.
- Verification of the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Information published on the GlobalSign web site.
- Any other services that GlobalSign might advertise or provide through its web site.

7.23.1 Reliance at Own Risk

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

7.23.2 Accuracy of Information

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

7.24 GlobalSign CA Obligations

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

- Comply with this CPS.
- Provide infrastructure and certification services, including the establishment and operation of the GlobalSign Repository and web site for the operation of public PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available.
- Issue digital certificates in accordance with this CPS and fulfil its obligations presented herein.
- Upon receipt of a request from an RA operating within the GlobalSign network act promptly to issue a GlobalSign certificate in accordance with this GlobalSign CPS.
- Upon receipt of a request for revocation from an RA operating within the GlobalSign network act promptly to revoke a GlobalSign certificate in accordance with this GlobalSign CPS.
- Revoke certificates according to this CPS.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Make a copy of this CPS and applicable policies available upon request.

GlobalSign acknowledges it has no further obligations under this CPS.

7.25 GlobalSign Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign network promises to:

- Receive applications for GlobalSign certificates in accordance with this GlobalSign CPS.
- Perform all verification actions prescribed by the GlobalSign procedures and this CPS.
- Receive, verify and relay to GlobalSign all requests for revocation of a GlobalSign certificate in accordance with the GlobalSign procedures and the GlobalSign CPS.

7.26 Limitation for Other Warranties

GlobalSign does not warrant:

- The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CPS and in the GlobalSign insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in PersonalSign 1, free, test or demo certificates.

7.27 Exclusion of Certain Elements of Damages

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

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on PersonalSign 1, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

7.28 Writings

Without prejudice to the requirements of the Directive 99/93 and national laws of the EU member states, GlobalSign acknowledges that 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.

7.29 Signatures

Without prejudice to the requirements of the Directive 99/93 and national laws of the EU member states, GlobalSign acknowledges that where there is a requirement for a signature or provision for certain consequences in the absence of a signature, that rule can be satisfied by a digitally signed message. In this regard, a signer must have the intention to sign such a message and the signature can subsequently be verifiable by reference to the public key listed in a valid certificate.

7.30 Fitness for a Particular Purpose

GlobalSign disclaims any warranty of fitness for a particular purpose.

7.31 Liability Caps

GlobalSign's aggregate liability to all parties is subject to the limits stated below under the GlobalSign Insurance Policy.

7.32 No Fiduciary Relationship

In no event does GlobalSign act as the agent, fiduciary, trustee or otherwise represents a GlobalSign partner, a subscriber or relying party. The relationship between GlobalSign and GlobalSign partners subscribers and that between GlobalSign and relying parties is not that of agent and principal. Neither GlobalSign partners nor subscribers or relying parties have any authority to bind GlobalSign, by contract or otherwise, to any obligation.

GlobalSign makes no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

7.33 Hazardous Activities

The GlobalSign public PKI services are not intended for use as control equipment in hazardous circumstances or for uses requiring foolproof performance including n uclear facilities, aircraft navigation or communication systems, air traffic control systems, weapons control systems etc. where failure could result in death, injury, or environmental damage.

7.34 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS prevails and bind the subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this CPS;
- Expressly superseding this CPS for which such contract is govern as to the parties thereto, and to the extent permitted by law.

7.35 Compliance with Export Laws and Regulations

Export of certain types of software used in certain GlobalSign public PKI products and services may require the approval of appropriate government authorities. Parties (including GlobalSign partners, subscribers and relying parties) agree to conform to applicable export laws and regulations.

7.36 Intellectual Property Rights

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

7.37 Infringement and Other Damaging Material

GlobalSign warrants that when subscribers submit to GlobalSign and use a domain name or a DNS they do not interfere with or infringe any 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. Parties also warrant that they do not intend to use such domain name and DNS for any unlawful purpose whatsoever

Certificate subscribers is indemnify without limitation GlobalSign for any loss or damage resulting from any such infringement.

7.38 Intellectual Property Licensing

Certificates are and remain pro perty of GlobalSign. GlobalSign permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that

certificates are not published in any publicly accessib le repository or directory without the express written permission of GlobalSign. The scope of this restriction is also intended to protect subscribers against the unauthorised republication of their personal data featured on a certificate.

7.39 Successors and Assigns

This CPS is binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties.

7.40 Severability

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

7.41 Notice

GlobalSign accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from GlobalSign the sender of the notice deem its communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:
GlobalSign, NV/SA,
Legal Practices,
Haachtsesteenweg 1426,
1130 Brussels,
Belgium.

7.42 Fees

GlobalSign may charge subscriber fees for the use of GlobalSign products and services. GlobalSign retains its right to effect changes to such fees.

7.43 Survival

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

7.44 Governing law

This CPS is governed by the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of GlobalSign digital certificates or other products and services. The law of Belgium applies also to all GlobalSign commercial or contractual relationships in which this CPS may apply or quoted implicitly or

explicitly in relation to GlobalSign products and services where GlobalSign acts as a provider, supplier, beneficiary receiver or otherwise.

7.45 Jurisdiction

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

7.46 Dispute resolution

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

7.46.1 Arbitration

If the dispute is not resolved within ten (10) days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code.

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

For all technology related disputes and disputes related to this CPS the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:
J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
tel.: +32-47-733 82 96
fax: + 32-16-32 54 38

8 GlobalSign Data Protection Policy

This part describes the specific Privacy conditions of data that GlobalSign collects.

8.1 Collected Information

GlobalSign public certification products and services are also intended to serve individuals. GlobalSign is committed to protecting the privacy of the applicants and subscribers of its public certification services. GlobalSign uses the personal information collected to process applications for digital certificates and provide a personalised service where possible.

8.2 Duty to Register

GlobalSign has registered with the competent authority in Belgium as required by law regarding its collecting, processing and archiving of personal data. You may refer to the competent authority named below to obtain further information regarding this registration:

Commissie voor de Bescherming van de Persoonlijke Levenssfeer Regentschapstraat 61	Commission pour la Protection de la Vie Prive rue de la Régence, 61	Commission for the protection of Personal Data r. de la Régence 61
1000 Brussel	1000 Bruxelles	1000 Brussels,
Belgie	Belgique	Belgium
Voice: +32 2 5427200 Fax: +32 2 5427212		

8.3 GlobalSign products

GlobalSign's public certification services, for which personal data may be collected and such warranties apply, include all types of certificates featured on its public web site as well as administrative certificates for GlobalSign RAs.

8.4 Follow relevant European and Belgian laws

GlobalSign commits to protecting the personal information applicants and subscribers of its public certification services submit. GlobalSign operates within the limits of the:

- European Directive 95/46 on *The protection of individuals with regard to the processing of personal data and on the free movement of such data.*
- Laws of Belgium regarding the protection of personal data
- Provisions of the GlobalSign CPS.

8.5 GlobalSign representations

GlobalSign represents to all applicants and subscribers that it follows the conditions below:

8.5.1 Legal Notice

GlobalSign makes practical efforts to provide notice to subscribers on the legal terms prevailing in the issuance of GlobalSign digital certificates. A published CPS and related agreements and information including but not limited to a Y2K statement, an insurance plan, a consumers statement, a relying parties agreement and this data protection statement are made available through the GlobalSign repository at: www.globalsign.net/repository.

8.5.2 Only PKI Services

GlobalSign makes available PKI based services and products while it makes no usage or retention of biometric or other means of identification or data.

8.5.3 Collecting Personal Data

GlobalSign only collects personal data that is necessary to verify an applicant's identity and issue digital certificates according to published and/or audited practices.

8.5.4 Proportionality

GlobalSign may only request the e-mail address and the name of an applicant or subscriber while for certain types of certificates including PersonalSign 2 certificates and PersonalSign 3 Pro certificates it may require additional information to be submitted, including an identification number, date of birth etc.

8.5.5 Payment Information

GlobalSign may collect credit card or other payment information from the applicants of its products and services as it sees appropriate to fulfil payment requirements. GlobalSign uses this information for payment purposes only, while it makes no further processing of it. GlobalSign maintains no paper records of the credit card records, while all relevant digital information is stored off-line. The submission and retention requirements of the credit card details do not apply to applicants of PersonalSign 1 or free, test and demo certificates.

8.5.6 Strict Identification Procedures

GlobalSign uses strict identification procedures to positively establish the identity of an applicant or subscriber. The procedures GlobalSign uses are either paper-based or electronic with a view to provide adequate assurances to relying parties about the identity of the subscriber.

8.5.7 Establish the Identity of the Subscriber

GlobalSign only collects personal data related to the core function of a PKI activity with a view to establish the identity of a subscriber and issue a digital certificate upon which parties may rely.

8.5.8 Redundant Data not Collected
GlobalSign collects no data revealing racial or ethnic origin, political opinions, religious and philosophical beliefs, trade-union membership or data concerning health or sex life.

8.5.9 Personally Submitted Data
GlobalSign only collects data directly from an applicant or subscriber or a duly authorised agent of theirs.

8.5.10 Legal Disclosures of Personal Data
GlobalSign only discloses personal data as required by law. Ahead of making such disclosures GlobalSign informs the applicant or subscriber of the requirement to effect such disclosures to the extent permitted by law or court order.

8.5.11 Trading Personal Data
GlobalSign does not sell, trade, exchange or otherwise make available to third parties personal information regarding applicants and subscribers unless so required by law.

8.5.12 No Escrow
GlobalSign uses no key escrow listing keys of the subscribers of its products or services. GlobalSign is only responsible for the good order of its own private key(s).

8.5.13 Personnel
All members of the GlobalSign personnel serving in trusted positions are of good standing and character including those members handling personal data. GlobalSign makes appropriate controls on the members of its staff with a view to deliver trustworthy PKI services.

8.5.14 Due authorisation
All members of the personnel of GlobalSign that handle personal data comply with Belgian Data Protection and Employment Law requirements to handle personal data lawfully.

8.5.15 Cookie Policy
GlobalSign might use non-intrusive cookie techniques to measure access to its web site and services. The function of GlobalSign as a Trust service provider does not necessarily coincide with intrusive practices that have been widely considered as monitoring the users of Internet based products and services.

8.5.16 Appended URLs
GlobalSign maintains the state of an applicant and subscriber of its services by appending a unique identification number to the URL in the browser of the applicant or subscriber. For an applicant or subscriber the clear advantage of using appended URLs as opposed to setting cookies is that information stored on its computer is deleted as soon as it exits the browser application. The applicant or subscriber stays firmly in control regarding the information it releases to the GlobalSign server.

8.5.17 Visitors

GlobalSign collects information on its www site from applicants of GlobalSign certificates or parties requesting PKI related products and services that GlobalSign makes available.

8.5.18 Links

GlobalSign may use links to other www sites as it sees appropriate. GlobalSign makes no representations regarding the protection of personal data offered in such web sites.

8.5.19 Independent CA

GlobalSign makes reasonable effort to remain an independent Trust service provider operating within the legal framework set out by the laws of the EU and Belgium.

8.5.20 Advertisment

GlogalSign only advertises on web sites that support a privacy policy compatible with the European Directive 95/46 on Data Protection.

8.5.21 Property

Personal data submitted by applicants and subscriber becomes and remains property of GlobalSign.

8.5.22 Trans-border Data Flows

GlobalSign operates a network of CAs, RAs and LRAs across Europe and beyond. Within this GlobalSign Network transmissions of personal data take place from the GlobalSign RAs and GlobalSign LRAs to GlobalSign where this data is finally processed and stored ahead of authorising issuing a certificate. Personal data flows within the GlobalSign network are directed from the RAs/LRAs to GlobalSign. GlobalSign neither supports nor performs any transmissions of personal data to countries other than the EU member states.

8.5.23 EU Level Privacy Protection

Historically, the Laws of the EU have been offering the highest level of personal data protection in the world. GlobalSign does not discriminate in providing personal data protection between users residing within the EU and others that do not. By allowing transmissions of personal data from countries with low or no data protection regulation to GlobalSign in Belgium, GlobalSign can effectively extend its EU level data protection policies to applicants and subscribers residing in countries outside the EU. Applicants and subscribers residing beyond the EU can therefore benefit from a higher data protection standard than what is offered in their own country of residence.

8.5.24 Pseudonyms

Following appropriate procedure, GlobalSign may issue pseudonym certificates upon request. Personal data revealing the identity of the pseudonym holder may be released to authorised parties as required by law.

8.5.25 Additional Personal Information
At the subscriber's request GlobalSign may include additional personal information on a certificate.

8.5.26 Scope of Collection of Personal Data
GlobalSign requests only personal data that is necessary to deliver a PKI related service.

8.5.27 Usage of Collected Data
GlobalSign pledges to decline from using submitted personal data for purposes other than what the original data had been collected for.

8.5.28 Beneficiary
The personal data that is requested from an applicant or subscriber of a GlobalSign product or service is essential to conclude an agreement of which applicants or subscribers are the immediate beneficiaries.

8.5.29 Consent Upon Submission
Upon submitting personal data the applicant or subscriber of GlobalSign products or services gives its consent for the submission and processing of data.

8.5.30 Commercial Announcements
GlobalSign may use contact information provided by an applicant or subscriber to circulate information regarding products, upgrades etc. Users or subscribers that do not desire to be notified so are encouraged to opt out appropriately on their registration form for GlobalSign services or products.

8.5.31 Administrative and Security Announcements
GlobalSign may use subscriber provided contact information to notify subscribers on administrative or security matters regarding GlobalSign products or services.

8.5.32 Forms of Publishing
GlobalSign uses paper-based and electronic communication material to appropriately explain the technology and the legal implications for the providers and the users of its products and services.

8.5.33 Multi-lingual Presentation
Although the culture of the web related services encourages the provision of information in English, through its extensive network of national alliance partnerships GlobalSign supports local languages for information and legal notice in the countries that it directly operates for issues including the protection of personal data.

8.5.34 Scope of Processing
Processing of personal data does not exceed the scope of the product or service offered, being the establishing of the identity of the applying or subscribing individual.

8.5.35 Personal Data Processing Systems
GlobalSign uses computer-based and manual filing systems to process personal data.

8.5.36 Processing and Transmission Equipment
GlobalSign uses equipment and applies appropriate procedures to transmit and store personal data.

8.5.37 Auditing Procedures
GlobalSign implements appropriate procedures to transmit and store personal data that may be audited as required by law or practice.

8.5.38 Plain Language
Wherever possible GlobalSign uses clear and plain language to adequately explain its legal position and policy regarding the provision of public certification services, including the protection personal data. GlobalSign also publishes explanatory statements, policy statements and promotional information on its www site.

8.5.39 Statistical and Other Processing of Personal Data
GlobalSign reserves its right to perform statistical, historical or scientific processing of the personal data it collects.

8.5.40 Application Assessment
GlobalSign examines applications for certificates and assesses them exclusively using criteria like data submitted and appropriate payments of the fees due. GlobalSign reserves the right to refuse to issue a certificate following appropriate examination and assessment of an application. Following the rejection of an application, an applicant may repeat the application process.

8.5.41 No Content Approval
As a provider of PKI products and services, GlobalSign is disassociated from the content and form of applications and content providers that use GlobalSign products or services. A GlobalSign certificate is not a sign of approval of the content of a message or a www site that uses it. Subscribers and users of GlobalSign products and services hold GlobalSign clear of any liability for damages, including consequential damages, as a result of treating personal data that is not included in a GlobalSign product or service and for which GlobalSign has not performed appropriate controls and/or treatment.

8.5.42 Subscriber Provided Information
Consistent with European and Belgian Laws regarding the provision of Trust services and the protection of personal data GlobalSign requests users to personally submit personal data. After performing appropriate computer-based and manual controls to ensure the accuracy of the submitted data, GlobalSign cannot accept any further responsibility for damages suffered because of inaccurate subscriber provided data except within the limits of GlobalCover: GlobalSign Insurance Plan, as explained below under art. 3.6.

8.5.43 Accessing Personal Data

Applicants and subscribers of GlobalSign products and services may contact GlobalSign to request accessing data that GlobalSign holds for them. Requests to access personal data are done through digitally signed e-mail or registered mail. GlobalSign's replies are sent within fifteen (15) business days from receipt of such request.

8.5.44 Accessing Personal Data

Applicants or subscribers whose data is kept by GlobalSign may contact GlobalSign to access and review data concerning them.

Rectifying personal data
If data held on a GlobalSign record is inaccurate or incomplete, GlobalSign completes or rectifies personal data from its records as appropriate, free of charge following a request from an applicant or subscriber.

Retention of personal data: Personal data submitted to GlobalSign will be retained for up to thirty (30) years or to the maximum period prescribed by law.

8.5.45 General Information Available

GlobalSign makes general information available on the www site with a view to provide background information including its line of products and services, Public Key Infrastructure, information security and the protection of personal data.

8.5.46 Other Statutory Rights

This statement does not affect any statutory or other rights private parties may have as data subjects or otherwise due to national law.

9 GlobalSign Consumer Policy Statement

This part describes the specific consumer related issues of GlobalSign public PKI services.

9.1 GlobalSign Products for Consumers

GlobalSign's public certification services for consumers include the following types of certificates:

- GlobalSign PersonalSign 2 Certificates,
- GlobalSign PersonalSign 3 Pro Certificates.

9.2 Follow European and Belgian Consumer Laws

GlobalSign promises to fully respect consumer rights as laid out in European and Belgian Law and operates within the limits of the:

- European Directives 93/13 on *Unfair Terms* and 97/7 on *The Protection of Consumers in respect of Distance Contracts*;
- Laws of Belgium regarding consumer protection;
- provisions of the GlobalSign CPS.

9.3 Equitable Approach

GlobalSign supports a viable legal relationship with the consumers undertaking several legal assurances and commitments.

9.4 Assurances of the Consumer

When applying for a certificate, consumers are asked to attest to the following statements that may also be required by law:

- the certificate applicant is the same as the person identified in the request;
- the certificate applicant rightfully holds the private key;
- the certificate applicant must make every effort to ensure that supplied information to be published in the certificate is accurate;
- for GlobalSign PersonalSign 2 certificates, authentication procedures include that the consumer mails or faxes a signed photocopy of an official identity document to a RA;
- for GlobalSign PersonalSign 3 Pro certificates, authentication procedures for consumers include the personal appearance of the applicant before a RA or a LRA for the proper registration of the applicant.

Following the successful issuance of a certificate a consumer is asked to provide GlobalSign with a few further assurances that may be required by law:

- there is an immediate relation between the private key and the public key published in the certificate of the subscriber and that the combination of both is the digital signature of the subscriber;

- the subscriber has duly kept the secrecy and integrity of its private key and no unauthorised persons had access to it;
- the subscriber makes truthful representations to GlobalSign;
- the subscriber promptly notifies GlobalSign when having notice of inaccuracies in the submitted information to be published in the certificate or kept by GlobalSign;
- the subscriber will only use a certificate for authorised and legal purposes for which it has been issued.

9.5 Assurances of GlobalSign

When issuing a certificate GlobalSign assures subscribers as follows:

9.5.1 European and Belgian Law

European and national laws impose obligations to suppliers of goods and services with regard to consumers. In this context, GlobalSign follows the directives of the EU and the national laws of Belgium regarding the protection of consumers.

9.5.2 Laws of Other EU Member States

GlobalSign makes efforts to co-ordinate its practices with consumer laws of other EU member states where it makes its services directly available through a GlobalSign Registration Authority.

9.5.3 Right to Be Informed

GlobalSign respects the right of consumers to be appropriately informed regarding the products and its public certification services. GlobalSign publishes all related information on its www site at www.globalsign.net.

9.5.4 Clear Language in Contracts

GlobalSign takes special care to present and explain in clear language the legal terms it publishes in the Certification Practice Statement or in other adjacent agreements.

9.5.5 Legal Notice

GlobalSign makes practical efforts to provide legal notice to subscribers on the legal terms concerning issuing GlobalSign digital certificates. A published CPS and related agreements and information including but not limited to a Y2K statement, an insurance plan, a privacy statement, a relying parties agreement and this consumer statement are made available through a dedicated www site at: www.globalsign.net/repository.

9.5.6 Plain Language

Although the provision of GlobalSign's public certification services is a highly technical subject in the non legally binding documentation GlobalSign uses clear and plain language to adequately explain its legal position and policy regarding the provision of public certification services. GlobalSign also publishes explanatory statements, policy statements and promotional information on its www site at www.globalsign.net while it makes available a helpdesk service for its subscribers.

9.5.7 Forms of Publishing

GlobalSign also uses additional paper-based or electronic communication material to explain the technology and the legal implications for the providers and the users of this technology.

9.5.8 Multi-lingual Presentation

Although the culture of the www-related services encourages the provision of information in English, GlobalSign through its extensive network of national alliance partnerships supports local languages for information and legal notice in the countries that it directly operates.

9.5.9 No Spamming

GlobalSign exclusively uses acceptable advertising methods and techniques.

9.5.10 Published Identity and Product Information

In accordance with European Legislation regarding the conclusion of distant contracts, GlobalSign clearly states all elements of its identity and specifications of its products and services, including pricing, delivery times, additional explanations etc.

9.5.11 Payment Information

GlobalSign uses plain e-mail and www information points to relay information to its users on arrangements concerning payment and delivery of the certificates or other related services.

9.5.12 Withdrawal Right

The consumer gets a “no questions asked” right of withdrawal from the transaction following 15 days after original delivery with full money back guarantee.

9.5.13 Right to Reject an Offer

Following original submission of the application to receive a certificate the consumer receives a 3-day validity period to assess the offer of GlobalSign on a “no questions asked” basis. No obligations are attached if a consumer never proceeds with its application.

9.5.14 Contract Duration Information

The typical duration of consumer contracts for the provision of certification services is 1 year with possible extension periods.

9.5.15 Accessing Information

GlobalSign makes every effort to keep information in its www site appropriately sorted and easily accessible.

9.5.16 Market Education

By distributing GlobalSign Class 1 Certificates free of charge, GlobalSign takes a pro-active stance regarding market education and testing of certificates by the users.

9.5.17 WWW Site

GlobalSign takes every effort possible to provide an easily accessible and comprehensive WWW site inclusive of all its services, products, policies as well as any other material related to these.

9.5.18 Strict Verification Procedures

GlobalSign uses strict verification procedures to establish the identity of the subscriber. The procedures GlobalSign uses are either paper-based or electronic with a view to provide adequate assurances to relying parties about the identity of the subscriber.

9.5.19 General Information Available

GlobalSign makes general information available on the www site with a view to provide background information on its line of products and services, Public Key Infrastructure and information security.

9.5.20 Insurance Plan

GlobalSign may also indicate reliance limits on the certificates it issues. For further information you may refer to *GlobalCover: GlobalSign Insurance Plan*.

9.5.21 Partners

To provide easier access to its services and reach out to the consumers GlobalSign supports an extensive network of national and regional partnerships.

9.5.22 New Products

In an effort to better respond to market needs and provide specialised services, GlobalSign reserves the right to make available new products and services, like usage constrained certificates (attribute certificates).

10 GlobalSign Insurance Policy

This part describes the specific conditions of the GlobalSign limited insurance scheme.

10.1 Beneficiaries of this Insurance Policy

10.1.1 Beneficiaries

This GlobalSign Insurance Policy Statement extends to the categories of individuals and/or legal persons (hereunder, beneficiaries) mentioned below. Without prejudice to the point of registration being a GlobalSign Registration Authority or a GlobalSign Local Registration Authority located anywhere in the world, beneficiaries are those that have successfully applied and received a valid certificate of the following classes or types:

- GlobalSign PersonalSign 2 certificate,
- GlobalSign PersonalSign 3 Pro certificate,
- GlobalSign ServerSign certificate,
- GlobalSign ObjectSign publishing certificate,
- GlobalSign HyperSign 128 certificates,
- GlobalSign ServerSign for WAP certificates,

10.1.2 Relying Parties

Some provisions of this Insurance Policy also apply to parties relying on GlobalSign certificates.

The indicated insurance limits are also suggested reliance limits for transactions effected by using a GlobalSign digital certificate.

10.1.3 Users of GlobalSign PersonalSign 1 Certificates

The GlobalSign Insurance Policy does not apply to users of GlobalSign PersonalSign 1 certificates, and to otherwise free and test certificates that GlobalSign might make available for purposes that include but are not limited to demonstration, education and testing.

10.1.4 Third Party Beneficiary Rights

This GlobalSign Insurance Policy is not intended to create any third party beneficiary rights for any person other than the parties described as beneficiaries in article 1 of this GlobalSign Insurance Policy Statement.

10.1.5 Unauthorised Products

The GlobalSign Insurance Plan coverage extends to parties that only purchase products or services directly from GlobalSign or through its accredited associates and partners located anywhere in the world. GlobalSign is not liable for and does not extend this GlobalSign Insurance Policy to parties that make use of unauthorised products that might bear the name GlobalSign.

10.1.6 Closed User Groups

This GlobalSign Insurance Policy does not apply to users of products or services purchased or otherwise made available for usage within aclosed user

group, which will be subjected to a separate agreement unless otherwise stated in the closed user group agreement.

10.1.7 GlobalSign Employees, Associates and Administrators:
This GlobalSign Insurance Policy also applies to all GlobalSign employees, associates and administrators of the GlobalSign network for certificates they receive for activities related to their line of work.

10.2 Scope of Coverage

10.2.1 Civil Liability Protection
This GlobalSign Insurance Policy Statement warrants that the core of GlobalSign's activities is subject to a civil liability protection plan. The GlobalSign Insurance Plan warrants against the risks associated with using a digital certificate mentioned under paragraphs 2.2 and 2.3.

10.2.2 Errors in the Identification Process
This GlobalSign Insurance Policy applies to any loss as a result of an error in the identification process that may be committed by any accredited member of the personnel of any GlobalSign Registration Authority and GlobalSign Local Registration Authority in the GlobalSign network including administrators, employees and trainees in the line of their professional activities or function.

10.2.3 Loss of Documents
This GlobalSign Insurance Plan covers the risk of loss of documents related to the identification process that an applicant submits to GlobalSign to establish its identity.

10.2.4 Intentional or Accidental Errors
This GlobalSign Insurance Policy warrants against intentional or accidental errors including libel and slander that might be committed by any member of the personnel of a GlobalSign Registration Authority or a GlobalSign Local Registration Authority.

10.2.5 Limited Warranty
This GlobalSign Insurance Policy Statement is a unilateral declaration of GlobalSign to assure the users of its digital certificates of the trustworthin ess of its products and procedures. This GlobalSign Insurance Policy Statement is not intended to be extended or interpreted towards any field of coverage or any scope other than those specifically described hereunder.

10.3 Exceptions

The following list of exceptions of liability of GlobalSign to refund a beneficiary for loss suffered is indicative to include but not be limited to the cases following in this article.

10.3.1 Honorary Rewards etc.
Claims related to disputes from honorary rewards, costs or commercial debts.

10.3.2 Refusal to Pay etc.
Liability arising from refusal to pay or refund cash, stock, titles, guarantees, except those foreseen under article 2 of this GlobalSign Insurance Policy Statement.

10.3.3 Civil Liability Burdens
Liability as a result of a particular obligation undertaken by a beneficiary that burdens their civil liability status, like statutory liability, and assumption of liability for a third party, contractual penalties etc.

10.3.4 Penalties or Punitive Damages
Compensation inflicted by judicial, transactional, fiscal, administrative, disciplinary or economic penalties or punitive damages or exemplary damages as well as judicial costs of a penal procedure when they burden a beneficiary personally.

10.3.5 Insolvency
Claims as a result of the insolvency of a beneficiary are excluded for this insurance policy statement that is not intended to offer cover coverage of the beneficiaries.

10.3.6 Control Over a Beneficiary
Claims imposed by any legal entity that has control over a beneficiary, any affiliate of a beneficia ry, any legal entity controlled by a beneficiary or its affiliates.

10.3.7 Collective Liability
If any of the beneficiaries that is deemed responsible for the facts leading to a liability claim is found in one of the exception positions explained above, the exception will be extended to the rest of the beneficiaries also.

10.3.8 Request for Revocation
Failure or unreasonable delay of the beneficiaries to properly dispatch a request for revocation of a GlobalSign certificate as required results in cancelling this GlobalSign Insurance Policy Statement.

10.3.9 Due Diligence
Failure of the beneficiaries to exercise due diligence to prevent compromise or loss of the subscriber's private key results in cancelling this GlobalSign Insurance Policy Statement.

10.3.10 Material Obligations of the CPS
Failure of the beneficiaries to comply with each and every material obligation under the CPS results in cancelling this GlobalSign Insurance Policy Statement.

10.3.11 Security Measures

Failure of the beneficiaries to apply reasonable security measures to verify the digital signature of a subscriber, a Registration Authority or a Local Registration Authority results in cancelling this GlobalSign Insurance Policy Statement.

10.3.12 Reasonable Security Measures

Any failure of the beneficiaries to apply reasonable security measures prior to and during the creation and further processing of encrypted messages addressed to a subscriber of a GlobalSign certificate for purposes of sharing confidential or secret data with such Subscriber as an intended recipient results in cancelling any rights emanating from this GlobalSign Insurance Policy Statement.

The foregoing is without prejudice to cases of:

- failure to determine that the subscriber's GlobalSign certificate is valid and
- failure to validate a certificate chain for a subscriber's GlobalSign certificate result in cancelling this GlobalSign Insurance Policy Statement.

10.3.13 Illegal Acts

Illegal acts by the beneficiaries being either a subscriber or a relying party result in cancelling this GlobalSign Insurance Policy Statement. The foregoing is without prejudice to illegal acts committed by a person -- including an *agent provocateur*-- coercing the beneficiaries to perform acts causing the beneficiaries loss or damages and which also result in cancelling this GlobalSign Insurance Policy Statement. GlobalSign may appropriately seek compensation for any damages suffered as a result of illegal acts of the beneficiary.

10.3.14 Misuse of Services

Any person causing damages or misusing the Internet, telecommunication or Value Added Networks (VAN) including usage or reproduction of computer viruses has no right to make a rightful claim from this GlobalSign Insurance Policy Statement.

The foregoing is without prejudice to persons attacking or otherwise interfering with:

- Reverse engineering, directly or indirectly.
- The technical implementation of any of the GlobalSign services.

The foregoing result in cancelling this GlobalSign Insurance Policy Statement unless permitted in writing by GlobalSign.

10.3.15 Reasonable Failure of Equipment

Reasonable failure of GlobalSign infrastructure or equipment does not result in cancelling this GlobalSign Insurance Policy Statement.

The foregoing is without prejudice to failure that lies outside GlobalSign's control, which are, however, essential for GlobalSign to perform in

conformance with its scope of operation including power or telecommunication failures out of the control of GlobalSign, which also create no right for a claim under this GlobalSign Insurance Policy Statement.

10.3.16 Failure of Hardware and Software Equipment

While GlobalSign carries no liability for failure of software or hardware developed outside its immediate sphere of influence it makes all reasonable efforts to utilise software and hardware equipment from recognised vendors and follow internationally recognised standards for its products and services.

10.3.17 Sensitive Equipment

All GlobalSign non-attribute certificates provided through its public certification services, are issued for general commercial usage. This GlobalSign Insurance Plan does not apply when certificates are used for the operation of sensitive equipment including but not limited to nuclear facilities, aircraft navigation or communication, air-traffic control systems, weapons control systems and at all cases that may result directly in death, personal injury or severe environmental damage.

10.3.18 Prior Authorisation

This GlobalSign Insurance Policy Statement does not apply to certificates issued without prior authorisation and where no payment has been received therefore, including delays in payment, unless otherwise agreed.

10.3.19 Limits

This GlobalSign Insurance Policy Statement is not intended to create any rights on issues beyond those described in this Statement.

10.3.20 Punitive Damages

Punitive damages are excluded from this insurance policy statement.

10.4 Field of coverage

10.4.1 Truthful Facts

Without prejudice to requirements set under exceptions in article 3.0 of this GlobalSign Insurance Policy Statement coverage extends to requirements that will be substantiated on the basis of facts inducing liability that are true.

10.4.2 Jurisdiction

In case of a lawsuit the coverage will be attributed if the beneficiaries prosecute in a court of justice in a jurisdiction other than the United States of America or Canada.

10.4.3 Other Claims

Contract or liability claims not related to a GlobalSign certificate are not covered by this GlobalSign Insurance Policy Statement.

10.4.4 Own Fault

Liability caused in part or in whole by a fault of the applicant as a result of his/her own breach of a warranty or obligation stated in the CPS or any other GlobalSign Insurance Policy Statement with GlobalSign makes void all claims for a refund under this insurance plan.

10.5 Temporal Validity of the Coverage

GlobalSign has no obligation to make a payment unless the beneficiary submits a payme nt request as described below.

10.5.1 Delays

All claims must be brought to the attention of GlobalSign without any delay and in a period of maximum 15 days from the discovery of the error or damages.

10.5.2 Insurance Period

The coverage for the documented claims must be brought before GlobalSign during the insurance period. Insurance period is the time between two expiry dates.

10.5.3 Extension of the Insurance Period

This GlobalSign insurance policy statement also covers written claims that reach GlobalSign in a period of 3 months following the end of the contract for the certificate. These claims must be based on damages that occurred during the period of coverage of the contract if coverage is not provided through another insurer.

10.5.4 Facts

Facts are considered introduced in the first insurance year of the first claim irrespectively of the time they were submitted.

10.6 Payment Requests

10.6.1 Incidental or Consequential Damages

The GlobalSign Insurance Plan will cover any incidental or consequential damages caused by a breach of theconditions set out in articles 2 and 3 observing the limits set out in article 7.0.

10.6.2 Procedure

A beneficiary must:
- send a written request for payment using a digitally signed electronic message, registered mail or courier service, without any delay.
-Work together with GlobalSign to establish the facts substantiating the claim and the parties involved.
-Subrogate to GlobalSign every and all claims it may have against third parties for damages that may eventually result in reimbursing GlobalSign for payments made to the beneficiary up to the amount paid by GlobalSign.

This insurance policy may be cancelled for reasons related to the appropriateness of the reaction of the beneficiary that include but are not limited to the following: delays to appropriately inform GlobalSign on the damages, deviations from the prescribe procedures, failure to subrogate claims.

10.7 Limitations on Payments for Subscribers

The GlobalSign Insurance Plan sets limits to the maximum amount GlobalSign may pay to a beneficiary even if damages exceed the amount set by GlobalSign. Limits are determined according to the class of the certificate as explained in the table below:

Maximum limits in the GlobalSign Insurance Plan for Subscribers(*)	
GlobalSign PersonalSign 2 Certificates	2500 EURO
GlobalSign PersonalSign 3 Certificates	37500 EURO
GlobalSign ServerSign Certificates	37500 EURO
GlobalSign ObjectSign Certificates	37500 EURO
GlobalSign HyperSign 128 Certificates	37500 EURO
GlobalSign ServerSign for WAP Certificates	37500 EURO

Damages exceeding the liability cap set for any given certificate shall be apportioned first to the earliest claims to achieve final resolution. GlobalSign may refuse to pay more than the total liability cap for each certificate, regardless of the method of apportionment among claimants of the amount of the liability cap. The foregoing is without prejudice to punitive damages. This section is limited by applicable law.

10.8 Limitations on Payments for Relying Parties

The GlobalSign Insurance Plan sets limits to the maximum amount GlobalSign may pay to a beneficiary relying party even if damages exceed the amount set by GlobalSign. Without prejudice to the provisions of article 10.1 (on Single Payment) GlobalSign limits the reliance limits to a certificate to the limits per category as set for subscribers, i.e. a maximum of 2500 EURO per GlobalSign class 2 certificates and 375000 EURO per certificate for all other categories. These limits are set and will be respected irrespective of the times that a certificate has been wrongly used.

Maximum limits in the GlobalSign Insurance Plan for Relying Parties(**)	
GlobalSign PersonalSign 2 Certificates	2500 EURO
GlobalSign PersonalSign 3 Certificates	37500 EURO
GlobalSign ServerSign Certificates	37500 EURO
GlobalSign ObjectSign Certificates	37500 EURO
GlobalSign HyperSign 128 Certificates	37500 EURO
GlobalSign ServerSign for WAP	37500 EURO

Certificates	

**As above under (*)

10.9 Limitation on Payment for Subscribers and Relying Parties

The liability caps provided under articles 8.0 and 9.0 will remain unchanged regardless of the number of digital signatures, transactions, or claims related to a certificate.

10.10 Other Limitations of Liability

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 any type of a GlobalSign certificate **except for information featured on PersonalSign 1, free, test or demo certificates (for which no warranties or obligations apply) t**hat 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 set by law. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions or claims associated with such certificate. In the event the liability cap be exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by court order. In no event shall GlobalSign 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.

10.11 Maximum Limits

Coverage per damage and per insurance year extends to the capital and the costs and interest.

Maximum limit is the maximum amount that GlobalSign may pay a beneficiary (a subscriber or a relying party) for any and all breaches of a limited warranty in the insurance period. Payments GlobalSign makes may ultimately reduce the amount available for future payments.

When the total amount allocated for insurance payments is exhausted, GlobalSign may have no further obligation to refund a beneficiary. This section is limited by applicable law.

New certificates issued to old users and renewed certificates all hold a new insurance period valid throughout their validity period as explained under art. 6.0.

10.12 Single Payment

GlobalSign certificates issued as a result of error and/or impersonation are deemed to constitute a single breach regardless of how many relying parties rely on that certificate.

Subscribers making usage of multiple certificates for the same transaction they may choose, following appropriate declaration by the means of art. 6.2 which certificates provide the insurance for this transaction.

10.13 Updates and Amendments

This GlobalSign Insurance Policy Statement as well as other agreements and policy statements related to the provision of GlobalSign's certification services may be updated from time to time. A beneficiary is responsible to monitor changes and obtain the latest version of this and other agreements and policy statements that apply in the provision of the service that it applies for. Agreements and policy statements become valid upon publication and they remain valid throughout the period they remain posted in the GlobalSign Repository governing all products and services distributed in that period.

10.14 Force Majeure

Force majeure condition under this GlobalSign Insurance Policy Statement and/or the CPS results in cancelling any rights emanating from this policy statement.

10.15 Conflict of Provisions

In case of conflict between this GlobalSign insurance policy statement and the CPS, the CPS prevail.

10.16 Severability

If any provision of this GlobalSign Insurance Policy Statement, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this GlobalSign Insurance Policy Statement (and the application of the invalid or unenforceable provision to other persons or circumstances) be interpreted so that it reasonably effects the intent of its parties.

Provisions of this GlobalSign Insurance Policy Statement that provide for a limitation of liability, 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.

10.17 Governing law

This GlobalSign Insurance Policy Statement is governed by Belgian Law.

10.18 Statutory rights

This GlobalSign Insurance Policy Statement does not affect any statutory rights of the subscriber emanating from European or national legislation, including consumer laws and data protection laws.

11 GlobalSign Products

This part describes the public GlobalSign products.

11.1.1 Personal Certificates

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

- **PersonalSign Demo™**: provides only an unambiguous e-mail address within the GlobalSign repository while GlobalSign performs no authentication of the identity of the applicant. **PersonalSign Demo™**: certificates are meant for test and demonstration purposes only and they are valid for 1 month.
- **PersonalSign 2™**: provides a limited identity authentication by requiring a signed copy of an identity proof. These personal digital certificates for browsers can be used for most low-value/low risk commercial transactions like online purchases. They are valid for one year.
- **PersonalSign 3™**: provides a high level of identity assurance by requiring that the applicant appears personally before a Registration Authority to prove its identity. These certificates can be used for high-value/high risk commercial transactions such as electronic banking. They are valid for one year.

11.1.2 Server Certificates

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

- **ServerSign™**: GlobalSign offers ServerSign™ for entities wishing to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in commercial and financial transactions. The identity of the ServerSign-holder is fully-authenticated by GlobalSign.
- **HyperSign128™**: is a server-level certificate which "enhances" SSL technology to deliver strong (128-bit) encryption in an internet browsing session. They address the need for additional security in especially sensitive electronic transactions or communications while, subject to US export rules, they are currently available to banks, financial institutions, insurance companies, health and medical organisations, online merchants and overseas subsidiaries of US companies.
- **ServerSign for WAP™**: GlobalSign makes available certificates for WAP gateways.

11.1.3 Object Publishing Certificates

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

- **ObjectSign™** ensures the identity of an entity that distributes software on the Internet, and guarantees the integrity of the software being

distributed as well, utilizing Microsoft Authenticode or Netscape's ObjectSigning standards. ObjectSign™ assures relying parties on the integrity of the message and verifies the identity of the sender of a software object to ensure that the certified software object originates from a trusted source.

11.2 Accepted Subscriber Names

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

11.2.1 Pseudonyms

For certain types of products GlobalSign may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law.

11.3 Validation

For all types of certificates GlobalSign reserves the right to update validation procedures and subscriber submitted data to improve the validation process. Further details concerning validations and updated validation procedures are included in the per product description in the chapters below and may also be obtained from GlobalSign, NV/SA, Haachtsesteenweg 1426, 1130 Brussels, Belgium, Attn. Legal Practices.

12 PersonalSign 1 Demo

This part describes the specific requirements for PersonalSign 1 certificates.

12.1 General

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

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

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

They are typically used 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). They are not intended for commercial use where proof of identity is required and should not be relied upon for such uses.

GlobalSign may use PIN protected encryption software to issue PersonalSign 1 demo certificates.

PersonalSign 1 demo certificates are intended for test purposes only.

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

PersonalSign 1 demo certificates are free of charge.

PersonalSign 1 demo certificates validity period is 30 days.

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

12.2 Assurance level

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

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

12.3 Individuals

A certificate request can be done according to the following means:
On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.
E-mail (S/MIME): The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

12.4 Content

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

- Applicant's e-mail address
- Applicant's public key
- Issuing certification authority (GlobalSign):
- GlobalSign digital signature
- Type ofalgorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

12.5 Certificate Profile

PersonalSign 1 Profile	
CN	GlobalSign Class 1 CA
O	GlobalSign NV/SA
OU	Class 1 CA
COUNTRY	BE
PERIOD	1 year
AUTHORITY KEY IDENTIFIER	Non Critical/Key Identifier
KEY USAGE	Critical 0xF0

NETSCAPE CERTIFICATE TYPE	Not Critical / 0xA0
BASIC CONSTRAINT	NO
CERTIIFCATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

12.6 Submitted documents to identify the applicant

No documents are required in association with a PersonalSign 1 demo certificate.

12.7 Time to confirm submitted data

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

12.8 Issuing procedure

The following steps describe the milestones to issue a PersonalSign 1 demo certificate:
1 The applicant fills out the online request on GlobalSign's website
2 The applicant submits the required information:
e-mail address
3 GlobalSign verifies the applicant's e-mail address by sending an e-mail with a URL where the applicant can start the registration procedure
4 The applicant fills out the registration form, as part of the online request
5 The applicant accepts the online subscriber agreement
6 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
7 The public key and the online request are sent to GlobalSign automatically.
8 GlobalSign authorises the issuance of a certificate
GlobalSign sends e -mail to the applicant with a URL that permits the applicant to retrieve the certificate.
9 GlobalSign publishes the issued certificate in on line database.
10 Renewal: not allowed
11 Revocation: allowed but remains at GlobalSign's descretion

12.9 Insurance

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

12.10 Relevant GlobalSign Legal Documents

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

2 Subscriber Agreement
3 Privacy Policy
4 Consumer Policy
5 Insurance Policy

13 PersonalSign 2

This part describes the specific requirements for PersonalSign 2 certificates.

13.1 General

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

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

GlobalSign uses PIN protected encryption software to issue PersonalSign 2.

PersonalSign 2 certificates validity period is 1 year.

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

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

PersonalSign 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.

13.2 Assurance Level

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

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

13.3 Individuals:

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

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

13.4 Content

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

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

13.5 Certificate Profile

PersonalSign 2 Pro Profile	
CN	GlobalSign Class 2 CA
O	GlobalSign NV/SA
OU	Class 2 CA
COUNTRY	BE
PERIOD	1 year
AUTHORITY KEY IDENTIFIER	Non Critical/Key Identifier
KEY USAGE	Critical 0xF0
NETSCAPE CERTIFICATE TYPE BASIC CONSTRAINT	Not Critical / 0xA0 NO
CERTIIFCATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

13.6 Documents Submitted to Identify the Applicant

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

13.7 Time to Confirm Submitted Data

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

13.8 Issuing Procedure

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

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

13.9 Insurance

GlobalSign accepts liability up to 100.000 BEF or 2500 EURO per damage caused by a false identity in a PersonalSign 2 certificate used according to the CPS

13.10 Relevant GlobalSign Legal Documents

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

1 CPS
2 Subscriber Agreement
3 Privacy Policy

4 Consumer Policy
5 Insurance Policy

14 PersonalSign 3 Pro

This part describes the specific requirements for PersonalSign 3 Pro certificates.

14.1 General

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

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

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

GlobalSign uses PIN protected encryption software to issue PersonalSign 3 pro. A cryptographic module is recommended but not required

PersonalSign 3 certificates validity period is 1 year.

14.2 Individuals

A certificate request can be done according to the following means:
On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.
E-mail (S/MIME): The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additio nal documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

14.3 Content

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

- Applicant's e-mail address
- Applicant's name

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

14.4 Certificate Profile

PersonalSign 3 Pro Profile	
CN	GlobalSign Class 3 CA
O OU	GlobalSign NV/SA Class 3 CA
COUNTRY	BE
PERIOD	1 year
AUTHORITY KEY IDENTIFIER	Non Critical/Key Identifier
KEY USAGE	Critical 0xF0
NETSCAPE CERTIFICATE TYPE	Not Critical / 0xA0
BASIC CONSTRAINT	NO
CERTIIFCATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

14.5 Documents Submitted to Identify the Applicant

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

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

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

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

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

14.6 Time to Confirm Submitted Data

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

14.7 Issuing Procedure

The following steps describe the milestones to issue a PersonalSign 3 certificate:

1 The applicant fills out the online request on GlobalSign's website
2 The applicant submits the required information:
e-mail address
3 GlobalSign verifies the applicant's e-mail address by sending an e-mail with a URL where the applicant can start the registration procedure
4 The applicant submits the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
5 The applicant accepts the on line subscriber agreement.
6 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
7 The public key and the online request are sent to GlobalSign automatically
8 GlobalSign verifies by personal appearance before LRA and checking articles of association, proof of professional context and payment
9 RA may positively verify the applicant.
10 GlobalSign may issue the certificate to the applicant.
11 GlobalSign publishes the issued certificate in on line database.
12 Renewal: allowed.
13 Revocation: allowed.

14.8 Insurance

GlobalSign accepts liability up to 1.500.000 BEF or 37500 EURO per damage caused by a false identity in a PersonalSign 3 certificate used according to the CPS.

14.9 Relevant GlobalSign Legal Documents

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

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

15 ServerSign

This part describes the specific requirements for ServerSign certificates.

15.1 General

ServerSign certificates are meant for secure communication with a web-site through an SSL link that allows for 40bit encryption.

The applicant is an organisation that has a web-site. Server certificates are used to assure the web-sites identity to the visitor and to assure a confidential communication with the web-site.

GlobalSign uses PIN protected encryption software to issue ServerSign certificates. A cryptographic module is recommended but not required

ServerSign certificates are issued to legal entities only.

15.2 Business Entities

A certificate request can be done according to the following means:
On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.
E-mail (S/MIME): The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

15.3 Content

Typical content of information published on a ServerSign certificate includes the following elements

- Applicant's domain name
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country

- Issuing certification authority (GlobalSign)
- GlobalSign digital signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

15.4 Certificate Profile

ServerSign Profile	
CN	GlobalSign Secure Server CA
O OU	GlobalSign NV/SA Secure Server CA
COUNTRY	BE
PERIOD	1 year
AUTHORITY KEY IDENTIFIER	Non Critical/Key Identifier
KEY USAGE	Critical 0xF0
NETSCAPE CERTIFICATE TYPE	Not Critical / 0x04
BASIC CONSTRAINT	NO
CERTIIFCATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

15.5 Documents Submitted to Identify the Applicant

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

15.6 Time to Confirm Submitted Data

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

15.7 Issuing Procedure

The following steps describe the milestones to issue a ServerSign certificate:

1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
2 The applicant follows the on line registration procedure.

3 The applicant submits the required information including organizational information, technical contact, server information, payment information.
4 The applicant accepts the on line subscriber agreement.
5 Data are sent with certificate request to GlobalSign automatically.
6 GlobalSign verifies the submitted information by checking organisational, payment and any other information as it sees fit also through third party databases or resources.
7 GlobalSign may positively verify the applicant.
8 GlobalSign may issue the certificate to the applicant.
9 GlobalSign publishes the issued certificate in online database
10 Renewal: allowed
11 Revocation: allowed

15.8 Insurance

GlobalSign accepts liability up to 1.500.000 BEF or 37500 EURO per loss due to a false identity in a certificate used following the CPS.

15.9 Relevant Globalsign Legal Documents

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

1 CPS
2 Subscriber Agreement
3 Insurance Policy

16 ObjectSign

This part describes the specific requirements for ObjectSign certificates.

16.1 General

ObjectSign certificates are used for the signing of objects, such as software and press a rticles.

GlobalSign uses PIN protected encryption software to issue ObjectSign. A cryptographic module is recommended but not required

ObjectSign certificates validity period is 1 year.

ObjectSign certificates are issued to legal entities and independents.

16.2 Business Entities

A certificate request can be done according to the following means:
On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.
E-mail (S/MIME): The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

16.3 Content

Typical content of information published on a Object Sign certrificate includes the following elements:

- Applicant's e-mail address
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign digital signature
- Type of algorithm

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

16.4 Certificate Profile

ObjectSign Profile	
CN	GlobalSign Object Publishing CA
O	GlobalSign NV/SA
OU	Object Publishing CA
COUNTRY	BE
PERIOD	1 years
PUBLIC KEY LENGTH	1024
AUTHORITY KEY IDENTIFIER	Non Critical/Key Identifier
KEY USAGE	Critical 0xF0
NETSCAPE CERTIFICATE TYPE	Not Critical / 0x010
BASIC CONSTRAINT	NO
CERTIIFCATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

16.5 Documents Submitted to Identify the Applicant

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

16.6 Time to Confirm Submitted Data

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

16.7 Issuing Procedure

The following steps describe the milestones to issue an ObjectSign certificate:

1 The applicant fills out the online request on GlobalSign's website
2 The applicant submits the required information:
e-mail address
3 GlobalSign verifies by checking e-mail address: GlobalSign sends e-mail with URL where the applicant can start the registration procedure
4 The applicant fills out the registration form: e-mail address, organizational info, common name, country code, payment info
5 The applicant accepts the online subscriber agreement

6 A key pair is generated on an applicant's device (e.g. computer, smart card device etc.)
7 The public key and online request are sent to GlobalSign automatically
8 GlobalSign verifies the submitted information by checking organisational, payment and any other information as it sees fit also through third party databases or resources.
9 GlobalSign may positively verify the applicant.
10 GlobalSign may issue the certificate to the applicant.
11 GlobalSign publishes the issued certificate in online database
12 Renewal: allowed
13 Revocation: allowed

16.8 Insurance

GlobalSign accepts liability up to a maximum of 1.500.000 BEF or 37500 EURO per loss due to a false identity in an ObjectSign certificate used following the CPS.

16.9 Relevant GlobalSign Legal Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.net/repository:
1 CPS
2 Subscriber Agreement
3 Insurance Policy
4 Data Protection Policy (if applicable)

16.9.1 GlobalSign Private Key Protection

GlobalSign's private key is secured against compromise via trustworthy hardware products.

16.9.2 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 cryptographic modules (such as smart cards or PC cards) as specified in this CPS.

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.

16.9.3 Possible Applications Supported

The examples listed in Table 2, above, simply reflect GlobalSign's model on 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 imply that a party has authority to act on behalf of another. Relying parties are exclusively responsible to verify a received

digital signature. A digital certificate does not grant any rights other than these described in this CPS.

17 HyperSign 128

This part describes the specific requirements for HyperSign 128 certificates.

17.1 General

HyperSign 128 certificates are meant for secure communication with a web site trough an SSL link that allows for 128-bit encryption.
HyperSign 128 certificates provide a high level of credibility for an organisational web site.

The applicant is an organisation that has a website and that is eligible to receive GlobalSign SGC server certificates under current U.S. policy on encryption export control as mentioned in the subscriber agreement that is available on www.globalsign.net/repository.
In principal HyperSign 128 certificates are currently available to:

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

17.2 Business Entities

A certificate request can be done according to the following means:
On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.
E-mail (S/MIME): The certificate applicant submits an appropriately formatted certificate request to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

17.3 Content

Typical content of information published in a HyperSign 128 certificate includes the following elements:

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

17.4 Documents Submitted to Identify the Applicant

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

17.5 Time to Confirm Submitted Data

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

17.6 Issuing Procedure

The following steps describe the milestones to issue a HyperSign 128 certificate:

1 The applicant proves its eligibility by electing the sector its organisation belongs to and submits server information.
2 The applicant creates a Certificate Signing Request (CSR) and a key pair using appropriate server software.
3 The applicant copies and paste its certificate signing request and submits.
4 The applicant confirms the information included in its certificate -signing request.
5 The applicant submits the required information including organizational information, technical contact, server information, and payment information.
6 The applicant verifies the organizational and payment information.
7 The applicant accepts the on line subscriber agreement.
8 Data are sent with certificate request to GlobalSign automatically.
9 GlobalSign verifies the submitted information by checking organizational, payment and any other information at it sees fit also trough third party databases or resources.
10 GlobalSign may positively verify the applicant.
11 GlobalSign may issue the certificate to the applicant.
12 GlobalSign publishes the issued certificate in online database.
13 Renewal: allowed.
14 Revocation: allowed.

17.7 Disclaimer

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

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

17.8 Insurance

GlobalSign accepts liability up to 1500000 BEF or 37500 EURO per loss due to a false identity in a certificate used following the CPS.

17.9 Relevant GlobalSign Legal Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.net/repository:
1 CPS
2 Subscriber Agreement
3 Insurance Policy

17.10 Documentation

Refer to the GlobalSign HyperSign 128/Secure Server SGC agreement.

17.11 Approval

GlobalSign has been granted approval to issue SGC server certificates (i.e. HyperSign 128) to certain classes of organizations for Microsoft Web Server Software, subject to export licenses issued by the United States Department of Commerce.

17.12 Applicant profile

Applicant represents that it is one of the following entities that are eligible to receive GlobalSign HyperSign 128 certificates under current U.S. policy on encryption export control.

18 ServerSign for WAP

This part describes the specific requirements for ServerSign for WAP certificates.

18.1 General

A ServerSign for WAP certificate enables of an organisation and enables end-users to verify the web site of the organisation and to communicate via state-of the-art WTLS encryption.

ServerSign for WAP certificates' validity period is 1 year.

ServerSign for WAP certificates are issued to legal entities only.

18.2 Content

Typical content of information published on a ServerSign for WAP certificate includes the following elements:

- Applicant's name of organisation
- Applicant's service name
- Applicant's public key
- Code of Applicant's country
- Issuing certification authority (GlobalSign)
- GlobalSign digital signature
- Type of algorithm
- Validity period of the digital certificate
- Optional: common name
  - www address or
  - IP address: public or private

18.3 Documents Submitted to Identify the Applicant

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

18.4 Time to Confirm Submitted Data

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

18.5 Issuing procedure

The following steps describe the milestones to issue a ServerSign for WAP certificate:

1 Applicant creates Certificate Signing Request (CSR).
2 Applicant follows on line registration.

3 Applicant submits the required information: organisational information, technical contact, server information, and payment information.
4 Applicant accepts the on line subscriber agreement.
5 Data are sent with certificate request to GlobalSign automatically.
6 GlobalSign verifies the submitted information by checking organizational, payment and any other information as it sees fit also trough third party databases orb resources
7 GlobalSign may positively verify the applicant.
8 GlobalSign publishes the issued certificate in online database.
9 Renewal: allowed.
10: Revocation: not allowed.

18.6 Insurance

GlobalSign accepts liability up to 1.500.000 BEF or 37.500 EURO per loss due to a false identity in a certificate used following the CPS.

18.7 Relevant GlobalSign Legal Documents

The applicant must take notice and is bound by the following documents available on www.globalsign.net/repository:
1 CPS
2 Subscriber Agreement
3 Insurance Policy

19 Root-sign certificates

This part describes the specific requirements for Root-sign certificates.

19.1 General

Root-sign certificate certificates invoke trust at the level of applications by allowing CAs to access popular applications through GlobalSign's trusted root that has been embedded in such applications.

The applicant is an organisation that operates a CA or is a CA.

GlobalSign recommends a cryptographic module is recommended to be used by the applying organisation.

Root-sign certificate certificates are issued to legal entities only.

19.2 Business Entities

A certificate request can be done according to the following means:
E-mail (S/MIME): The certificate applicant submits an appropriately formatted certificate request (PKCS#10) to GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign of any inaccuracy or defect in a certificate or earlier notice of informational content to be included in the certificate.

19.3 Content

Typical content of information published on a Root-sign certificate includes the following elements:

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

19.4 Documents Submitted to Identify the Applicant

Following the signing of a Root-sign agreement, the applicant must submit to GlobalSign directly a signed registration form, a signed subscriber agreement and the articles of association of the applying organisation.

19.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames. For Root-sign certificate verification might require up to 15 working days.

19.6 Issuing Procedure

The following steps describe the milestones to issue a Root-sign certificate:

1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
2 The applicant submits a request (PKCS#10).
3 The applicant submits the required information including organizational information, technical contact and any other information.
4 Data are sent with certificate request to GlobalSign.
5 GlobalSign verifies the submitted information by checking organisational, any other information as it sees fit also through third party databases or resources.
6 GlobalSign may positively verify the applicant.
7 GlobalSign may issue the certificate to the applicant.
8 GlobalSign publishes the issued certificate in online database.
9 If GlobalSign detects any problem in the application of the subscriber it informs this subscriber accordingly.
10 Renewal: allowed
11 Revocation: allowed

19.7 Insurance

GlobalSign extends a conditional insurance plan to selected Root-signed CAs it has validly entered a Root-sign agreement with. For such CAs GlobalSign accepts liability of up to 250000 EURO per loss for the accuracy of the subscriber CA information included in the Root-sign certificate.

19.8 Relevant Globalsign Legal Documents

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

1 CPS
2 GlobalSign Root-sign agreement

20 Definitions

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.
ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.
APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to an CA to issue a digital certificate.
ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.
ASSURANCES
A set of statements or conduct aiming at conveying a general intention.
AUDIT
Procedure used to validate compliance with formal criteria or controls.
AUTHENTICATED RECORD
A signed document containing assurances of authentication or a message with a digital signature verified by a valid Class 3 certificate by a relying party.
AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and veryfying such relationship.
AUTHORISATION
Granting of rights.
AVAILABILITY
The rate of accessibility of information or resources.
BINDING
A statement by an RA of the relationship between a named entity and its public key.
CERTIFICATE CHAIN
A hierarchical list certificates containing an end-user subscriber certificate and CA certificates.
CERTIFICATE EXPIRATION
The end of the validity period of a digital certificate..
CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.
CERTIFICATE HIERARCHY
A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.
CERTIFICATE MANAGEMENT
Actions associated with certificate management include, storage, dissemination, publication, revocation, and suspension of certificates.
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to me consulted by relying parties at all times prior to relying on information featured in a certificate.
CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA.
CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital certificate.
CERTIFICATION
The process to issue a digital certificate.
CERTIFICATION AUTHORITY (CA)
An authority, such as GlobalSign that issues, suspends, or revokes a digital certificate.
CERTIFICATION PRACTICE STATEMENT (CPS)
A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a certificate.
COMMERCIAL REASONABLENESS
A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.
COMPROMISE
A violation of a security policy that results in loss of control over sensitive information.
CONFIDENTIALITY
The condition to disclose data to selected and authorised parties only.
CONFIRM A CERTIFICATE CHAIN
To validate a certificate chain in order to validate an end-user subscriber certificate.
CRYPTOGRAPHIC ALGORITHM
A mathematical process that produces a prescribed result.

CRYPTOMODULE
A cryptosystem that performs encryption and decryption of data.
DIGITAL CERTIFICATE
A formatted piece of data that relates an identified subscriber with a public key he uses.
DIGITAL SIGNATURE
To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.
DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.
ELECTRONIC DATA INTERCHANGE (EDI)
The interchange of data message structured under a certain format between business applications.
E-MAIL (ELECTRONIC MAIL)
Messages sent, received or forwarded in digital form via a computer-based communication mechanism.
ENCRYPTION
To transform plain data in text format to an unintelligible form in such a way 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 CA subscriber other than another CA.
ENHANCED NAMING
The usage of an extended organisation field (OU=) in an X.509 v.3.0 certificate.
EXTENSIONS
Extension fields in X.509 v.3.0 certificates.
GENERATE A KEY PAIR
A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.
GLOBALSIGN PUBLIC CERTIFICATION SERVICES
A digital certification system made available by GlobalSign as well as the entities that belong to the GlobalSign network of CAs as 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 according to the rules defined by X.509 for that extension type.
GLOBALSIGN PROCEDURES
A document describing GlobalSign's internal security procedures.
HASH
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:
- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION
The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.
INCORPORATE BY REFERENCE
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.
KEY GENERATION PROCESS
The trustworthy process of creating a private/public key pair. The public key is supplied to an CA during the certificate application process.
KEY PAIR
A private key and its corresponding public key in asymmetric encryption.
(LOCAL) REGISTRATION AUTHORITY (LRA)
An entity (organisation) appointed by a CA to perform the registration and approval applications for digital certificates. An (L)RA is trusted to register other entities and assign them a relative distinguished value such as a distinguished name or, a hash of a certificate that is unambiguous within that domain.
NON VERIFIED SUBSCRIBER INFORMATION

Information submitted by a certificate applicant to an CA, and published in 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. Such information includes titles, professional degrees, etc.

NOTICE

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

NOTIFY

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

OBJECT IDENTIFIER

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

PersonalSign 1, 2, OR 3 CERTIFICATE

A certificate of a specified level of trust as defined by GlobalSign.

PKI HIERARCHY

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

PRIVATE KEY

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

PUBLIC KEY

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

PUBLIC KEY CRYPTOGRAPHY

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

PUBLIC KEY INFRASTRUCTURE (PKI)

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

RELATIVE DISTINGUISHED NAME (RDN)

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

RELIANCE

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

RELYING PARTY

A recipient who acts in reliance on a certificate and digital signature.

REPOSITORY

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

REVOKE A CERTIFICATE

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

SECRET SHARE

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

SECRET SHARE HOLDER

An person that holds a secret share.

SECRET SHARE ISSUER

A person that creates and distributes secret shares, including a CA.

SECURITY POLICY

A document on the requirements and practices maintained by a trustworthy system.

SIGNATURE

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

SIGNER

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

SMART CARD

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

SUBJECT OF A DIGITAL CERTIFICATE

The holder of a private key corresponding to a public key.

SUBSCRIBER

The subject of a digital certificate that uses the private key that corresponds to the public key listed in the certificate.

SUBSCRIBER AGREEMENT

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

SUSPEND A CERTIFICATE

A temporary make a digital certificate inoperable.

TIMESTAMP

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

TRUSTED POSITION

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

TRUSTWORTHY SYSTEM

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

WAP – WIRELESS APPLICATION PROTOCOL

A protocol for mobile communications.

WEB -- WORLD WIDE WEB (WWW)

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

WRITING

Information accessible and usable for reference.

X.509

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

A Document Control and References

GlobalSign NV/SA
Haachtsesteenweg 1426 Chaussée de Haecht, B-1130 Brussels, Belgium

URL: *http://www.globalsign.net*
E-mail: *info@globalsign.net*
Phone: *+32 (0) 2 7243636*
Facsimile: *+32 (0) 2 7243637*

Copyright Notice

Changes forecast

This is the final version 4.0. No more changes are expected for v.4.0