In support of GlobalSign public PKI services

GlobalSign Certificate Policy

Version 1.0
Publication Date: 15 March 2002

Approved by the GlobalSign Policy Management Authority

Contents

Acknowledgments

GlobalSign acknowledges the work of:

- IETF RFC 2527
- X.9.79 of the American Bankers Association
- Qualified Certificate Policy ETSI TS 101 456 of the Specialist Task Force 155 of the European Telecommunications Standards Institute (ETSI);
- PKI Assessment Guidelines, Information Security Committee of the American Bar Association.

1 Introduction

This CP applies to all public services of GlobalSign. This CP 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.

This CP complies to the formal requirements of IETF RFC 2527 with regard to format and format. While certain section titles are included according to to the structure of RFC 2527, the topic may not necessarily apply in the implementation of the PKI services of GlobalSign. Such sections are indicated as "Section not applicable".

This CP has formally been reviewed for compliance with CP requirements as mandated by certain accreditation schemes. Further information on compliance with such schemes can be obtained from GlobalSign, attn. Legal Practices, Philipssite 5, B-3001 Leuven, Belgium.

1.1 Overview

This CP aims at facilitating the GlobalSign network in delivering PKI services. This CP applies to all CAs, RAs and LRAs in the GlobalSign network.

GlobalSign accepts comments regarding this CP addressed to: legal@globalsign.net or by post to GlobalSign, attn. Legal Practices, Philipssite 5, B-3001 Leuven, Belgium.

1.2 Document Name and Identification

This GlobalSign CP may also utilise an OID.

1.3 PKI participants

1.3.1 GlobalSign Certification Authority

A Certification Authority is an organisation that issues digital certificates that are used in the public domain or within a business or transactions context. 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 requires appropriate publication in a certificate revocation list. GlobalSign operates such a list.

1.3.1.1 GlobalSign Certification Authority and GlobalSign CA 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.

1.3.2 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, notifying 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 GlobalSig n 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.

1.3.3 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.

1.3.4 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.

1.3.5 Other participants

GlobalSign may act as a certificate manufacturing entity for GlobalSign partners. Additionally it may provide repository services to other entities that provide PKI-related services.

1.4 Certificate usage

Certain limitations apply to the usage of GlobalSign certificates.

1.4.1 Appropriate certificate usage

GlobalSign certificates can be used for most electronic commerce transactions and mobile commerce transactions that support PKI such as electronic mail, retail transactions, contracts, accessing web sites and other online content etc.

1.4.2 Prohibited certificate usage

Certain limitations to the usage of GlobalSign certificates are stated in the GlobalSign CPS. A PersonalSign 1 Demo certificate for example does not provide any assurances regarding the identity of the subscriber while it can be used for encryption of data.

1.5 Policy Administration

The GlobalSign Policy Managing Authority manages this CP. GlobalSign is responsible for the registration, maintenance, and interpretation of this CP.

As an operator of a Trust network, GlobalSign approves of other CAs that enter its network of Trust. Such approval is established on the basis of an audit performed on the CP or CPS or both (if available) of such partner. GlobalSign can be contacted with regard to such third party CP or CPSs documentation.

To approve of a third party CP or CPS and establish the level of relevance to the GlobalSign CP or CPS GlobalSign takes the following steps:

1. Establish contractual relationship
2. Define business framework and project context

3. Provide the third party with an audit report on a number of essential points that include but are not limited to the following:
   - CA contact information
   - Certificate type, validation procedures and usage
   - Reliance limits and limitations of liability
   - Obligations of parties involved in the certificate life cycle
   - Certificate status-checking
   - Registration procedures
   - CA, RA, LRA model
   - Applicable agreements, Certificate
   - Privacy policy
   - Applicable law, complaints and dispute resolution
4. Accredit the third party CA

Any policy approved by GlobalSign has to ultimately comply with the provisions of the CP.

1.6 Definitions and acronyms

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

2 Publication And Repository Responsibilities

GlobalSign publishes information about the digital certificates it issues in (an) online repository(ies). GlobalSign reserves its rights to publish certificate status information on third party repositories.

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

PKI participants are notified that GlobalSign may publish information they submit to it on publicly accessible directories in association with digital certificate status information.

Due to their sensitivity GlobalSign refrains from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the functioning of *inter alia* its registration authorities, root sign procedures etc.

GlobalSign publishes digital certificate status information in frequent intervals as indicated in its CPS.

2.1 Access control on repositories

While GlobalSign strives to keep access to its public repository free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc.

While the access of GlobalSign CP, CPS policies, practices and procedures largely remains free of charge, GlobalSign retains its right to charge fees for otherspecific policy usage otherwise.

3 Identification and Authentication

GlobalSign maintains documented practices and procedures to authenticate the identity and/or other attributes of an end-user certificate applicant to a GlobalSign CA or GlobalSign RA prior to issuing a certificate.

GlobalSign uses approved procedures and milestone criteria to accept applications from entities seeking to become GlobalSign CAs, RAs, or other entities operating in or interoperating with a PKI.

GlobalSign authenticates the requests of parties wishing the revocation of certificates under this policy.

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

3.1 Naming

To identify a subscriber GlobalSign follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names.

When applying for a GlobalSign certificate, the applicant's name must be meaningful unless explicitly permitted in the relevant product description and the GlobalSign CPS. GlobalSign issues certificates to applicants submitting a documented application containing a verifiable name.

Certain types of certificates, such as European Qualified Certificates issued according to the European Directive 99/93 may, however, be issued against a pseudonym linked to a meaningful name that GlobalSign keeps in its archives.

GlobalSign does not issue anonymous certificates to subscribers.

Names assigned to subscribers of a certificate are unique within the domain of the GlobalSign CA as they are always used together with a sequential number.

GlobalSign does not accept trademarks, logos or otherwise copyrighted graphic or text material for inclusion in its certificates.

3.2 Initial Identity Validation

For the identification and authentication procedures of the initial subscriber registration for each subject type (CA, RA, subscriber, or other participant) GlobalSign takes the following steps:

The subscriber identified in the subject field must prove possession of the private key corresponding to the public key being registered with GlobalSign. Such a relationship can be proved by, for example, a digital signature in the certificate request message.

GlobalSign requirements for the identification and authentication for organisations applying for a GlobalSign certificate include but are not limited to consulting third party databases that identify organisations or inspecting an organisation's articles of incorporation.

Applicant organisations include but are not limited to other CAs, (third party) RAs, subscriber (in the case of certificates issued to organizations or devices controlled by an organization), or other corporate participants.

For the identification and authentication for individual subscriber organisations applying for a GlobalSign certificate (CA; RA; subscriber (in the case of certificates issued to organizations or devices controlled byan organization), or other participant) a GlobalSign RA may take steps that include but are not limited to:

- Controlling documents such as identity cards, passport, driver's license
- Authenticating the identity of the organization or individual based on the documentation or credentials provided;
- Request for certain classes of certificates, an individual to physically appear before a GlobalSign RA at some stage before a digital certificate is issued.
- Applying additional requirements for applicant organisations such as duly signed authorisation documents or a corporate identification badge.

In certain cases GlobalSign may include "non-verified subscriber information" in a certificate it issues. Such information may include a professional status or job title etc. GlobalSign disclaims any and all liability with regard to publishing such non-verified subscriber information.

When GlobalSign includes information indicating authority such as specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate GlobalSign may request a specific written permission from the involved organisation.

GlobalSign accepts other CAs wishing to enter its own network and operate under its own hierarchy. Following an initial assessment and the signing of a specific agreement with GlobalSign the applicant CA has to provide GlobalSign with certain identification documents including an authorisation letter, articles of association. GlobalSign retains its right to consult third party databases that identify organisations in this regard.

3.3 Identification and Authentication for Re-key Requests

Section not applicable

3.4 Identification and Authentication for Revocation Requests

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

For all CAs, subject CAs, RAs, subscribers or other participants there is a continuous obligation to inform GlobalSign of all changes in the information featured in a certificate during the operational period of such certificate. Other obligations may additionally apply.

4.1 Certificate Application

Certificate applicants have the responsibility to provide accurate information on their certificate applications.

Regarding subscriber certificate applications GlobalSign requires that the applicant subscriber to be either that individual or his legal representative submit a certificate application.

Subscribers undergo an enrolment process with GlobalSign or a GlobalSign partner that requires:

- Filling out an application form.
- Generating a key pair, directly or through an agent.
- Delivering the generated public key corresponding to a private key to GlobalSign.
- Demonstrating to GlobalSign that the applicant has possession of the private key corresponding to the public key it submits to GlobalSign.
- Accepting the subscriber agreement.

GlobalSign partner certificates are issued pursuant to an agreement the GlobalSign and the perspective partner execute against identification data supplied by the partner at the stage of contracting. Additional information on credentials can be supplied at later stages with the subsequent requirement to have firstly revoked and then reissued related certificates. Supplied credential information is related to the type of CA/RA certificate issued.

GlobalSign partner certificates are issued pursuant to an agreement the GlobalSign and the perspective partner enter. CA and RA certificates are issued against data supplied at the stage of contracting. Additional credential information can be supplied at later stages with the subsequent requirement to have revoked and reissued the related certificates. Supplied credential information is related to the type of CA/RA certificate issued.

Associated or root signed CAs have this responsibility themselves for their own range of RAs.

4.2 Certificate Application Processing

After receiving an applicant's application the GlobalSign CA or RA or an associated CA or RA may perform identification and authentication procedures to validate the certificate application.

Subsequently, the GlobalSign CA or RA and an associated CA or RA either approve or reject the certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

A GlobalSign CA or RA and an associated CA or RA must act on and process a certificate application within a time frame of 7 working days.

4.3 Certificate Issuance

Following submission of a certificate application or a certificate renewal request a GlobalSign RA approves or disapproves the submitted information.

Following approval of the certificate application the GlobalSign RA approves the certificate application or it denies the Certificate application.

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

A GlobalSign CA verifies the identity of GlobalSign partners on the basis of credentials presented.

A GlobalSign CA retains its right to reject the application or an applicant of CA/RA certificates.

Following approval of credentials presented a GlobalSign CA issues the certificate to the partner CA/RA according to GlobalSign Key Generation Procedure.

4.4 Certificate Acceptance

An issued GlobalSign certificate is deemed accepted by the subscriber when any of the following conditions apply:

- Acknowledgement of acceptance by sending an email to support@globalsign.net.
- Use the standard online form where applicable.
- Use the certificate for the first time.
- Fifteen days lapse from issuance.

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

The GlobalSign CA posts issued certificate to an X.500 or LDAP repository. It also reserves its right to notify the certificate issuance by the GlobalSign CA to other entities for example, sending the certificate to the RA.

4.5 Key Pair and Certificate Usage

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

4.5.1 Subscriber

The obligations of the subscriber include:

4.5.1.1 Subscriber responsibilities

Unless otherwise stated in this CP or the GlobalSign CPS, subscribers are responsible for:

- Having knowledge of and, if necessary, seeking training on using digital certificates and PKI.
- Generating securely their private key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with GlobalSign.
- Ensuring that the public key submitted to GlobalSign corresponds to the private key used.
- Ensuring 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 the 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 the GlobalSign CPS.
- Notifying GlobalSign or a GlobalSign RA of any changes in the information submitted.
- Ceasing to use a GlobalSign certificate if any featured information becomes invalid.
- Ceasing to use 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 supervising agents or partners that apply for or use a GlobalSign certificate on behalf of the subscriber.
- Controlling the data agents submit to GlobalSign and notifying GlobalSign of any misrepresentation and omission made by an agent.

4.5.1.2 Subscriber Liability Towards Relying Parties

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

4.5.1.3 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 CP and any other conditions of usage that GlobalSign may make available by means of a subscriber agreement or a relying party agreement. Additionally parties demonstrate acceptance of the conditions of usage of the CP 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. Using GlobalSign Repositories can:

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

4.5.1.4 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 takes 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.

4.5.1.5 Subscriber Indemnification

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 attend 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.**

4.5.2 Relying party

The obligations of a relying party are as follows: .

4.5.2.1 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 CP 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 may be reasonable under the circumstances.

4.5.2.2 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 CP and any other conditions of usage that GlobalSign may make available. Parties demonstrate acceptance of the conditions of usage of the CP 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.

Using GlobalSign Repositories can:

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

4.5.2.3 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 takes 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.

4.6 Certificate Renewal

Certificate renewal means issuance of a new certificate to the subscriber without changing the subscriber's public key or any other information in the certificate.

Renewal is permitted between 30 days up until 7 working days from the expiration date of a certificate.

For end-user subscriber certificate the same public key can be used to issue a certificate up to three (3) consecutive times in total, allowing for a total length of three (3) years of the same key pair to be used. Beyond that time limit the same key pair may not be used any longer.

The subscriber may directly request the certificate renewal by logging in to a GlobalSign partner web site. A GlobalSign RA or CA does not directly renew subscriber certificates unless they receive a subscriber request.

The GlobalSign CA issues a new certificate following user authentication through a password or log in with the still valid certificate. For personal certificates GlobalSign requests logging with a still valid certificate. For organisational certificates GlobalSign request logging with a password.

The remainder of the procedures remain as in the initial registration process including:

- Notification of the new certificate to the subscriber;
- Conduct constituting acceptance of the certificate;
- Publication of the certificate by the CA; and
- Notification of certificate issuance by the CA to other entities.

Renewal of CA/RA certificates is subject to contractual arrangements between GlobalSign and GlobalSign partners or among GlobalSign partners.

4.7 Certificate Re-key

Not applicable.

4.8 Certificate Modification

Not applicable.

4.9 Certificate Revocation and Suspension

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 CP.
- The performance of a person's obligations under this CP 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 must at all times contact a GlobalSign RA to request suspension or revocation. Such contact can take place online or by non-digital channels. 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 CP. Verification of the identity can be done through information elements featured in the identification data the subscriber has submitted to the GlobalSign RA. The GlobalSign CA takes prompt action to revoke the certificate.

Relying parties must use on line resources that GlobalSign make available through its repository to check the status of certificates on which they wish to rely. GlobalSign CRLs are updated frequently with minimum intervals of three hours.

Upon partner request GlobalSign gives access to OCSP resources and a web site to which status inquiries can be submitted.

Relying parties must comply with GlobalSign policy and in specific with relying party obligations as published in this CP or the GlobalSign CP.

Suspension of GlobalSign certificates is supported.

Request for suspension can be submitted by a subscriber or a GlobalSign RA. In the case of an end-user subscriber certificate by means of a digitally signed message from subscriber or RA.

4.9.1 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 evidence of such conditions a subscriber may request the re-activation of a certificate.

GlobalSign publishes notices of suspended or revoked certificates 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 acertificate, 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.

4.10 Certificate Status Services

GlobalSign makes available certificate status checking services.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

Not applicable.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

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

5.1 Physical Security Controls

GlobalSign implements physical controls on its own premises including the following:

GlobalSign secure premises are located in an area appropriate for high-security operations. There are numbered zones and locked rooms, cages, safes, and cabinets.

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

Power and air conditioning operate with a high rate redundancy.

Premises are protected from any water exposures.

Prevention and protection and measures against fire exposures are implemented.

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

Waste disposal is controlled.

GlobalSign implement a partial off-site backup.

5.2 Procedural Controls

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

GlobalSign obtains a signed statement from each member of the staff on not having conflicting, confidentiality, privacy protection.

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

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

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

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

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

- Criminal convictions for serious crimes;
- Misrepresentations by the candidate;
- Appropriateness of references;
- Any clearances if available.

5.3.2 Background Checks and Clearance Procedures

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

5.3.3 Training Requirements and Procedures

GlobalSign makes available training for their personnel to perform their CA and RA work functions.

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

5.3.5 Job Rotation
Not applicable.

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

5.3.7 Controls of independent contractors
Independent contractors are subject to the same privacy protection and confidentiality conditions as GlobalSign personnel.

5.3.8 Documentation for initial training and retraining
GlobalSign Partners make available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

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

GlobalSign records events that include but are not limited to certificate lifecycle operations, attempts to access the system, and requests made to the system.

GlobalSign stores real-time audit logs, which are subsequently processed and archived on a weekly basis. Following an alarm or anomalous event the Network Administrator is notified.

Audit logs can only be viewed by authorised personnel including the Security Officer.
GlobalSign implements audit log back up procedures.

The audit log accumulation system is internal to GlobalSign.

Subject which caused an audit event to occur are not notified of the audit action.

GlobalSign performs vulnerability assessments from time to time.

5.5 Records Archival

GlobalSign's general records retention policies, include the following:

5.5.1 Types of records

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

5.5.2 Retention period

GlobalSign retains in a trustworthy manner records of GlobalSign digital certificates for a term as indicated in the GlobalSign CP.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

Not applicable.

5.5.5 Requirements for Time-stamping of Records

Not applicable.

5.5.6 Archive Collection

The GlobalSign archive collection system is internal.

5.5.7 Procedures to obtain and verify archive information

To obtain and verify archive information GlobalSign partners maintain records under clear hierarchical control and a definite job description.

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.

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.

5.6 Key Changeover

Not applicable.

5.7 Compromise and Disaster Recovery

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

GlobalSign strives to re-establish a secure environment taking inter alia steps that include, but are not limited to, revoking corrupted or suspected of being corrupted entity's certificate. Subsequently GlobalSign may re-issue a new certificate to the entity.

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

5.8 CA or RA Termination

Before terminating its CA activities, a GlobalSign Partner:

- Provides subscribers of valid certificates with reasonable notice of its intention to cease acting as a CA.
- Revokes all certificates that are still unrevoked or unexpired at the end of the 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 CP.
- If possible, it provides succession arrangements for the re-issuance of Certificates by a successor CA under the same CP.

6 TECHNICAL SECURITY CONTROLS

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

6.1 Key Pair Generation and Installation

6.1.1 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.

6.1.1.1 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 (other CAs). Other usages are restricted.

6.1.1.2 GlobalSign Private Key Type

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

For its primary key GlobalSign makes use of the MD5/RSA algorithm with a key length of 2048 bits and a validity period of 10 years.

For its operational key GlobalSign makes use of the MD5/RSA algorithm with a key length of 1024 bits and a validity period of 5 years.

6.1.2 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 CP. GlobalSign acknowledges public, international and European standards on trustworthy systems.

6.1.3 GlobalSign Key Generation Devices

The generation of the private key of GlobalSign occurs within a secure cryptographic device meeting appropriate requirements including ISO 15782-1, FIPS 140-1 level 3, ANSI X9.66.

6.1.3.1 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.

6.1.4 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.

6.1.4.1 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 member of the management makes authorisation of key storage and assigned personnel in writing.

6.1.4.2 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.

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

6.1.4.4 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.

6.1.5 GlobalSign Private Key Distribution

GlobalSign documents its own private key distribution and has the ability to alter the distribution of tokens in case token custodians need to be replaced in their role of token custodians.

6.1.6 GlobalSign Private Key Destruction

GlobalSign private keys are destroyed at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

GlobalSign keys are destroyed by shredding their primary and backup storage CD-ROMs, by deleting their shares and by powering off any hardware modules the keys are stored on.

Key destruction process is documented and associated records are archived.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

Such devices meet the requirements of FIPS PUB 140-1 Level 3 or higher, which guarantees, amongst other things, that any device tampering is immediately detected; and private keys cannot leave devices unencrypted

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting. A key protection mechanisms reporting document template is given in Appendix A

HSMs do not leave GlobalSign's premises. In case HSMs require maintenance or repair, which cannot be done within GlobalSign's premises, they are securely shipped to their manufacturer. Between usage sessions HSMs are kept within GlobalSign's secure premises (security perimeter A, B or C).

The GlobalSign CAs private key remains under *n* out of *m* multi-person control.

The GlobalSign CA private key is not escrowed.

At the end of a key generation ceremony, new CA keys are burnt encrypted on a (backup key storage) CD-ROM. GlobalSign records each step of the key backup process using a specific form for logging information.

The GlobalSign CA private key is locally archived within GlobalSign premises.

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

The GlobalSign CA private key can be destroyed at the end of its lifetime.

6.3 Other Aspects of Key Pair Management

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

6.4 Activation Data

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

6.5 Computer Security Controls

GlobalSign implements computer security controls.

6.6 Life Cycle Security Controls

GlobalSign performs periodic development controls and security management controls.

6.7 Network Security Controls

GlobalSign maintains a high-level network of systems security induding firewalls. Network intrusions are detected.

6.8 Time-stamping

Not applicable.

7 CERTIFICATE AND CRL PROFILES

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

7.1 Certificate Profile

GlobalSign publishes the certificate profiles it uses in its CPS.

7.2 CRL Profile

In conformance with IETF PKIX RFC 2459 GlobalSign supports CRLs compliant with:

- Version numbers supported for CRLs; and
- CRL and CRL entry extensions populated and their criticality.

The profile of the GlobalSign Certificate Revocation List is showing in the table below:

Version	[Version 1]	
Issuer Name	CountryName=[Root Certificate Country Name], organizationName=[Root Certificate Organisation], commonName=[Root Certificate Common Name] [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 3 hours]	
Revoked Certificates	*CRL Entries*	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

7.3 OCSP Profile

GlobalSign OCSP profile follows IETF PKIX RFC2560 OCSP v1. No OCSP extensions are supported. GlobalSign supports multiple certificate status requests in one OCSP request as long as they are signed by the same CA. The OCSP response is signed by a CA cross-certified OCSP root.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

GlobalSign performs periodic audits of its infrastructure including a WebTrust for CAs Audit. GlobalSign follows the schedule of WebTrust with regard to aspects of the audits that include:

- Period
- Content
- Identity and/or qualifications of the personnel performing the audit.

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

9 OTHER BUSINESS AND LEGAL MATTERS

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

9.1 Fees

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

Communication of fees is done through the web site of GlobalSign Partners or by contract where applicable.

9.1.1 Refund policy

GlobalSign implements a conditional refund policy as described in its Limited Warranty Plan.

9.2 Financial Responsibility

GlobalSign maintains insurance coverage for its liabilities as described in its limited warranty plan available under www.globalsign.net/repository

GlobalSign accepts no further liability beyond coverage under its limited warranty plan.

9.3 Confidentiality of Business Information

GlobalSign observes personal data privacy rules and confidentiality rules as described in the GlobalSign CP.

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.

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

9.4 Privacy of Personal Information

GlobalSign Partners make available a specific Privacy Policy for the protection of personal data of the applicant seeking a GlobalSign or a GlobalSign Partner certificate that they make available through their web site and/or their CP or CPS.

9.5 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 CP.

9.6 Representations and Warranties

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

Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

9.6.1 Subscriber Obligations

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

- Having knowledge and, if necessary, seeking training on using digital certificates and PKI.
- Generating securely their private key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with GlobalSign.
- Ensuring that the public key submitted to GlobalSign corresponds to the private key used.
- Ensuring 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 CP 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 CP.
- Notifying GlobalSign or a GlobalSign RA of any changes in the information submitted.
- Ceasing use a GlobalSign certificate if any featured information becomes invalid.
- Ceasing to use a GlobalSign certificate when it becomes invalid.
- Remove server certificates when invalid 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 issuedcertificate 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 anyGlobalSign directory any material that contains statements that violate any law or the rights of any party.
- Requesting the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a GlobalSign certificate.
- Appropriately supervising 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.

9.6.2 Relying Party Obligations

A party relying on a GlobalSign certificate promises to:

- Have knowledge of the use of digital certificates and PKI.
- Receive notice of the GlobalSign CP 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.

9.6.3 Subscriber Liability Towards Relying Parties

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

9.6.4 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 CP and any other conditions of usage that GlobalSign may make available. Parties demonstrate acceptance of the conditions of usage of the CP 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. GlobalSign Repositories include or contain :

- 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.

9.6.4.1 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 takes 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.

9.6.4.2 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 CP and the GlobalSign insurance policy.

9.6.5 GlobalSign CA Obligations

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

- Comply with this CP and its amendments as published under www.globalsign.net/repository.
- 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 CP and fulfil its obligations presented herein.
- Notify subscribers via email that certificates have been generated for them and how subscribers may retrieve certificates.
- Notify the applicant if GlobalSign is unable to validate the subscriber application according to this CP.
- 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 CP.
- 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 CP.
- Revoke certificates issued according to this CP upon receipt of a valid request to revoke a certificate from a person authorised to request revocation.
- Publish accepted certificates in accordance with this CP.
- Provide support to subscribers and relying parties as described in this CP.
- Provide for the expiration and renewal of certificates according to this CP.
- Publish CRLs on a regular basis in accordance with this CP.
- Notify relying parties of certificate revocation by publishing CRLs on the GlobalSign repository.
- Make a copy of this CP and applicable policies available upon request.

GlobalSign acknowledges it has no further obligations under this CP.

9.6.6 GlobalSign Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign network promises to:

- Receive applications for GlobalSign certificates in accordance with this GlobalSign CP.
- Perform all verification and authenticity actions prescribed by the GlobalSign procedures and this CP.
- Submit to GlobalSign the applicant's request in a signed message (certificate request).
- Record all actions in an event journal.
- Receive, verify and relay to GlobalSign all requests for revocation of a GlobalSign certificate in accordance with the GlobalSign procedures and the GlobalSign CP.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CP.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 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 CP and in the GlobalSign insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in PersonalSign 1, free, test or demo certificates.

9.7.2 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 CP.
- 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.

9.8 Limitations of Liability

The total liability of GlobalSign is limited in accordance with the provisions of the GlobalSign Limited Warranty Plan that sets specific limits to each class of GlobalSign products and services. The GlobalSign Limited Warranty Plan is published in the GlobalSign CP.

9.9 Indemnities

This section contains the applicable inmdemnities.

9.9.1 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.**

9.10 Term and Termination

This CP remains in force until notice of the opposite is communicated by GlobalSign on its repository under ww.globalsign.net/repository.

Notified changes are appropriately marked by an indicated version. Changes are applicable 30 days after publication.

9.11 Individual notices and communications with participants

Individuals communications made to the GlobalSign CA must be addressed to: legal@globalsign.net or by post to GlobalSign, attn. Legal Practices, Philipssite 5, B-3001 Leuven, Belgium.

9.12 Amendments

Minor changes to this CP that do not materially affect the assurance level of this CP are indicated by version number that contains a decimal number e.g. version 1.1 for a version with minor changes as opposed to version 2.0 that addresses major issues.

Minor changes to this GlobalSign CP do not require a change in the CP OID or the CP pointer (URL). Major changes that may materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CP pointer qualifier (URL).

The GlobalSign Policy Management Authority decides on the numbering of versions.

9.13 Dispute Resolution Procedures

GlobalSign refers to arbitration all disputes related to this CP.

9.13.1 Arbitration

If the dispute is not resolved within ten (10) days after initial notice pursuant to CP, 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 CP the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:
J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
tel.: +32-47-733 82 96
fax: + 32-16-32 54 38

9.14 Governing Law

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

9.15 Compliance with Applicable Law

GlobalSign complies with applicable law in Belgium. 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 as pertaining in Belgium.

9.16 Miscellaneous Provisions

Various provisions are applicable in relation with GlobalSign certificates as found under Section “Legal” in the GlobalSign CP and CPS.

10 List of definitions

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.

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

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

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

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

AUDIT
Procedure used to validate compliance with formal criteria or controls.

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

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

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.

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 CP.

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 a 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 CP.

NOTIFY
To communicate specific information to another person as required by this CP 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.

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.

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.

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

Philipssite 5
B-3001 Leuven, Belgium

URL: *http://www.globalsign.net*
E-mail: *info@globalsign.net*

Phone: *+32 (0) 16 28 71 23*
Facsimile: *+32 (0) 16* 28 74 04

Copyright Notice

Copyright © GlobalSign NV/SA 2002. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of GlobalSign NV/SA.

Requests for any other permission to reproduce this GlobalSign document (as well as requests for copies from GlobalSign) must be addressed to:

GlobalSign NV/SA
Philipssite 5
B-3001 Leuven - Belgium
E-mail: legal@globalsign.net

The trademarks “GlobalSign” and “BelSign” are registered trademarks of GlobalSign NV/SA.

Changes forecast

This is the final version 1.0. No more changes are expected for v.1.0