



## Contents

Acknowledgments	9
1. Introduction	10
Structure of this CPS	10
Example case of using this CPS	11
CPS and CP	11
Conformance to this CPS	12
GlobalSign conforms to this CPS and obligations found in adjacent agreements published on a GlobalSign repository. Comments	12
2. General	13
GlobalSign	13
Digital Certificates	13
Applicability of digital certificates	14
GlobalSign digital certificate range	14
Business Partnerships	14
Secure Devices and Private Key Protection	15
Selecting a Certification Service	15
Operational Controls	15
Gender References	15
3. Parties of GlobalSign PKI Services	16
GlobalSign Certification Authority	16
GlobalSign Certification Authorities and Partners	16
GlobalSign Registration Authorities and Local Registration Authorities	16
Subscribers	17
Relying Parties	17
4. Technology	18
Digital Certificate Management	18
Types of GlobalSign Certificates	18
Extensions and Naming	18
GlobalSign Directories and Repository	20
Standards Used for GlobalSign Certificate Requests	20
Subscriber Identification	21
Software and Hardware Devices	21
GlobalSign Private Key Generation Process	21
GlobalSign Key Generation	21
GlobalSign Private Key Storage	22
GlobalSign Private Key Distribution	22
GlobalSign Private Key Destruction	23
5. Organisation	24
GlobalSign Infrastructure	24
Organisational Good Standing	24
Compromise and Disaster Recovery	24

Trustworthy Systems	25
Termination of CA Operations	25
Accreditation of Entities	25
GlobalSign Accreditation	25
Financial Resources	25
Limited warranties	25
Compliance Documentation	25
Form of Records	26
Records Retention	26
Audit Logging Procedures	26
Logs for Core Functions	27
Audit for Core Functions	27
Availability of GlobalSign Certificates	28
Publication	28
Confidentiality Information	28
Secure Facilities	29
Contingency Plans and Disaster Recovery	29
Personnel Management and Practices	29
Publication of Information	30
<b>6. Practices and Procedures</b>	<b>31</b>
Certificate Application Requirements for Subscribers	31
Validation Information for Certificate Applications	31
Requirements to Validate Certificate Applications	32
Time to Confirm Submitted Data	33
Approval and Rejection of Certificate Applications	33
Certificate Issuance and Subscriber Consent	34
GlobalSign Representations Upon Certificate Issuance	34
Certificate Validity	35
Certificate Acceptance by Subscribers	35
Publication of Issued Certificates	36
Verification of Digital Signatures	36
Effect of Validating a Subscriber Certificate	37
Reliance on Digital Signatures	37
Certificate Suspension and Revocation	37
Certificate Renewal	38
<b>7. Legal Conditions of Issuance</b>	<b>39</b>
Representations of GlobalSign	39
Public Services Only	39
Information Incorporated by Reference in a Digital Certificate	39
Pointers to Incorporate by Reference	39
GlobalSign policy revision procedure	39
Acceptance of Updated Versions of the CPS	40
Displaying Liability Limitations, and Warranty	40
Disclaimers	40
Publication of Certificate Data	40
Monitoring the Accuracy of Submitted Information	40
Interference with a GlobalSign Implementation	41

Compliance with Software Standards	41
Root Signing Partnerships	41
Renewal	42
Secret Shares	42
Choice of Cryptographic Methods	43
Reliance on Non Verified Digital Signatures	43
Refusal to Issue a Certificate	43
Public Keys of Refused Applications	43
Subscriber Obligations	43
Indemnity	44
Relying Party Obligations	44
Subscriber Liability Towards Relying Parties	45
GlobalSign Repository and Web site Conditions	45
GlobalSign CA Obligations	46
GlobalSign Registration Authority Obligations	46
GlobalSign Repository Obligations	47
Limitation for Other Warranties	47
Exclusion of Certain Elements of Damages	47
Writings	47
Signatures	47
Fitness for a Particular Purpose	47
Liability Caps	48
No Fiduciary Relationship	48
Hazardous Activities	48
Conflict of Rules	48
Compliance with Applicable Laws	48
Compliance with Export Laws and Regulations	48
Intellectual Property Rights	48
Infringement and Other Damaging Material	48
Intellectual Property Licensing	49
Successors and Assigns	49
Severability	49
Notice	49
Fees	49
Survival	50
Governing law	50
Jurisdiction	50
Dispute resolution	50
<b>8. GlobalSign Data Protection Policy</b>	<b>51</b>
Collected Information	51
Duty to Register	51
GlobalSign products	51
Follow relevant European and Belgian laws	51
GlobalSign representations	52
<b>9. GlobalSign Consumer Policy Statement</b>	<b>58</b>
GlobalSign Products for Consumers	58
Follow European and Belgian Consumer Laws	58
Equitable Approach	58
Assurances of the Consumer	58

Assurances of GlobalSign	59
10. GlobalSign Limited Warranty Policy	62
Beneficiaries of this limited Warranty Policy and definitions	62
Scope of Coverage	63
Exceptions	63
Field of coverage	66
Temporal validity of the coverage	67
Payment Requests	67
Limitations on Payments for Subscribers	68
Limitations on Payments for Relying Parties	68
Limitation on Payment for Subscribers and Relying Parties	69
Maximum Limits	69
Single Payment	70
Updates and Amendments	70
Force Majeure	70
Conflict of Provisions	70
Severability	70
Governing law	70
Statutory rights	71
11. GlobalSign Products	72
Acceptable Subscriber Names	73
Validation	73
12. PersonalSign 1 Demo	74
General	74
Assurance level	74
Individuals	74
Content	75
Certificate Profile	75
Submitted documents to identify the applicant	76
Time to confirm submitted data	76
Issuing procedure	76
Limited Warranty	76
Relevant GlobalSign Legal Documents	76
13. PersonalSign 2	78
General	78
Assurance Level	78
Individuals:	78
Content	79
Certificate Profile	79
Documents Submitted to Identify the Applicant	80
Time to Confirm Submitted Data	80
Issuing Procedure	80
Limited Warranty	80
Relevant GlobalSign Legal Documents	81
14. PersonalSign 2 Pro	82

General	82
Individuals	82
Content	83
Certificate Profile	83
Documents Submitted to Identify the Applicant	83
Time to Confirm Submitted Data	84
Issuing Procedure	84
Limited Warranty	84
Relevant GlobalSign Legal Documents	85
<b>15. PersonalSign 3</b>	<b>86</b>
General	86
Individuals:	86
Content	87
Certificate Profile	87
Documents Submitted to Identify the Applicant	87
Time to Confirm Submitted Data	88
Issuing Procedure	88
Limited Warranty	88
Relevant GlobalSign Legal Documents	88
<b>16. PersonalSign 3 Pro</b>	<b>89</b>
General	89
Individuals	89
Content	90
Certificate Profile	90
Documents Submitted to Identify the Applicant	90
Time to Confirm Submitted Data	91
Issuing Procedure	91
Limited Warranty	91
Relevant GlobalSign Legal Documents	92
<b>17. ServerSign</b>	<b>93</b>
General	93
Business Entities	93
Content	93
Certificate Profile	94
Documents Submitted to Identify the Applicant	94
Time to Confirm Submitted Data	94
Issuing Procedure	94
Limited Warranty	95
Relevant GlobalSign Legal Documents	95
<b>18. ObjectSign</b>	<b>96</b>
General	96
Business Entities	96
Content	96
Certificate Profile	97
Documents Submitted to Identify the Applicant	97
Time to Confirm Submitted Data	97
Issuing Procedure	97

Limited Warranty	98
Relevant GlobalSign Legal Documents	98
<b>19. HyperSign 128</b>	<b>100</b>
General	100
Business Entities	100
Content	101
Documents Submitted to Identify the Applicant	101
Time to Confirm Submitted Data	101
Issuing Procedure	101
Disclaimer	102
Limited Warranty	102
Relevant GlobalSign Legal Documents	102
Documentation	102
Approval	102
Applicant profile	102
<b>20. ServerSign for WAP</b>	<b>103</b>
General	103
Content	103
Documents Submitted to Identify the Applicant	103
Time to Confirm Submitted Data	103
Issuing procedure	103
Limited Warranty	104
Relevant GlobalSign Legal Documents	104
<b>21. Root-sign certificates</b>	<b>105</b>
General	105
Business Entities	105
Content	105
Documents Submitted to Identify the Applicant	106
Time to Confirm Submitted Data	106
Issuing Procedure	106
Limited Warranty	106
Relevant Globalsign Legal Documents	106
<b>22. Definitions</b>	<b>107</b>





## **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.
- AICPA/CICA WebTrust Program for Certification Authorities.



## **1. Introduction**

*This section gives a brief introduction to the GlobalSign CPS.*

This CPS applies to all public services directly delivered or made available by GlobalSign. This CPS comprises the parts included in the Table of Contents as well as any other documents or versions of 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 CPS also applies to selected branded services delivered by GlobalSign's partners who rely on GlobalSign to deliver digital certificates. While such partners operate their own GlobalSign accredited entities to issue self-branded or co-branded certificates GlobalSign provides the back end infrastructure and support for such services. In these circumstances GlobalSign accredited entities act as CAs; hence all responsibilities associated with the GlobalSign CA as specified in this CPS apply to them.

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 relevant European Union (EU) and Belgian regulations this CPS also comprises GlobalSign's Privacy, Consumer and Insurance policies to give a more detailed view of the level of service currently made available by GlobalSign.

This CPS is complemented by a Certificate Policy that addresses the needs and requirements of the GlobalSign network of partners.

### **Structure of this CPS**

This CPS contains a "General Part" and a "Specific Per-product Part".

The "General Part" addresses the conditions of issuance of digital certificates applicable to all products. The General Part is organised along Chapters 1 through to 10 to address technical organisational and legal matters associated with the usage of PKI and digital certificates. The choice of the structure is based on the typical breakdown of electronic commerce and information security matters to create a logical relation between the subject in question and its reference within this CPS. Rather than opting for a procedural approach, that appeals to PKI experts, this CPS allows the reader to associate a technical matter for example with its reference in Chapter 4. Hence, readers that are not as familiar with the various aspects of PKI can more easily navigate through this document and extract the information necessary.

The "Specific Per-product Part" addresses conditions associated with specific GlobalSign products. This per product part is organised along the product lines that GlobalSign makes available. While the major assurances remain shared among the whole range of GlobalSign products, there are certain procedure and contractual differences that create the various levels in the GlobalSign product range. Such differences are addressed on a per-product basis.



The following table gives an overview of the content of organisation of the various chapters in the GlobalSign CPS and describes the relationship among the various parts of it:

GlobalSign Certification Practice Statement		
<b>General Part</b>		
Parties of GlobalSign PKI services		
Technology		
Organisation		
Practices and Procedures		
Legal Conditions		
Data protection Policy		
Consumer Policy		
Insurance Policy		
<b>Specific Part</b>		
Products Policies		
Product 1	Product 2	Product x

This CPS comprises of all PKI products that GlobalSign makes available. Hence, there is no need to opt for an additional CPS for other families of products. This approach reflects the high level assurance that GlobalSign's own infrastructure warrants, that is shared among all categories of its products.

To use this CPS correctly the reader must refer to the general part and to the part specific to the product it purchases.

### 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 for the issuing of 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 he or she would have to turn to section 10.

### CPS and CP

This CPS is complemented by a GlobalSign CP. The purpose of the GlobalSign CP is to state the "what is to be adhered to (the rules)", and is generally defined by the entity wishing to ensure a level of trust through the use of certificates.

This CPS states "how the Certification Authority adheres to the Certificate Policy" (i.e. a summary of the processes and procedures the Certification Authority will use in creating and maintaining the certificate).



## **Conformance to this CPS**

### **GlobalSign conforms to this CPS and obligations found in adjacent agreements published on a GlobalSign repository.**

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



## **2. General**

*This section describes the GlobalSign certification services.*

### **GlobalSign**

GlobalSign operates under two roles. Firstly, as a Trust Service Provider to directly or through an agent deliver Trust Services to the user community. An agent in this case are third party Registration Authorities (RAs) that operate under agreement with GlobalSign.

Secondly GlobalSign operates an international network of Trusted Third Parties (TTP's) sharing the GlobalSign procedures and using suitable brand name to issue high quality and highly trusted digital certificates to public and private entities. Such partners include GlobalSign accredited Certification Authorities (CAs) and RAs that operate under an agreement with GlobalSign.

The main activities of GlobalSign are to:

- Set up and manage an international network of CAs and RAs, establishing the brand name of GlobalSign as a universal Trusted Third Party in PKI.
- Set up and manage third party PKIs on behalf of third party partners for outsourced PKI projects.
- Provide 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.

### **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.



### Applicability of digital certificates

GlobalSign makes available general-purpose digital certificates that can be used for non-repudiation, authentication and encryption. Usage of these certificates can be further limited to a specific business context. By means of an agreement with third parties GlobalSign may provide for such limitations of usage.

For example, a GlobalSign RA that operates within the health sector may issue certificates to health professionals that can only be used within their business context.

### GlobalSign digital certificate range

The range of GlobalSign digital certificates to which this CPS applies, includes the following products as described in chapters 11 etc. of this CPS.

GlobalSign products addressed in this CPS		
<b>PersonalSign Demo</b>	<i>A personal certificate of low assurance</i>	<i>Reference Chapter 13</i>
<b>PersonalSign 2</b>	<i>A personal certificate of medium assurance</i>	<i>Reference Chapter 14</i>
<b>PersonalSign 2 Pro</b>	<i>A personal certificate of medium assurance with reference to professional context</i>	<i>Reference Chapter 15</i>
<b>PersonalSign 3</b>	<i>A personal certificate of high assurance</i>	<i>Reference Chapter 16</i>
<b>PersonalSign 3 Pro</b>	<i>A personal certificate of high assurance with reference to professional context</i>	<i>Reference Chapter 17</i>
<b>ServerSign</b>	<i>A certificate for web servers</i>	<i>Reference Chapter 18</i>
<b>ObjectSign</b>	<i>A certificate for data objects</i>	<i>Reference Chapter 19</i>
<b>HyperSign 128</b>	<i>A certificate for web servers with high encryption level</i>	<i>Reference Chapter 20</i>
<b>RootSign</b>	<i>A certificate for CAs that enter the GlobalSign hierarchy</i>	<i>Reference Chapter 21</i>

### Business Partnerships

To respond better 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.



### **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.

### **Selecting a Certification Service**

While GlobalSign currently offers a broad 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 and use their own judgement before applying for a GlobalSign certificate.

### **Operational Controls**

GlobalSign undertakes 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.

### **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 community associated with the lifecycle of GlobalSign public PKI services.*

#### **GlobalSign Certification Authority**

A CA is an organisation that issues digital certificates. GlobalSign is a CA. Sometimes, a CA is also described by the term Issuing Authority.

GlobalSign is responsible for drafting the policy prevailing in issuing a certain type or class of digital certificates, including its public certificates. GlobalSign is also a Policy Authority while this CPS and the associated GlobalSign CP are policy that apply in issuing 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 (CRL). GlobalSign operates such a list.

#### **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 (including a Certificate Policy and/or Certificate Practice Statement).

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 (issuing CA certificates) of CAs to facilitate interoperability and invoke trust while providing widespread acceptance and trust of the certificates of a third-party CA.

Third parties can operate GlobalSign supported CAs and RAs to act as providers of public services or within the context of their own professional relationships on approval and authorisation by GlobalSign. GlobalSign CAs act in accordance with GlobalSign's practices and procedures. There is no limitation to the number of CAs that may be associated with GlobalSign either directly or through a third party relationship. If required GlobalSign provides CAs with the necessary technology and know-how to obtain a high level of training in accordance with GlobalSign accreditation requirements.

#### **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.

### **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.

### **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 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.*

### **Digital Certificate Management**

GlobalSign certificate management, in general, 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.

### **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.

### **Extensions and Naming**

#### **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.



### **Digital Certificate Extensions**

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

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

As key usage extension limits the technical purposes for which a public key listed in a 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 proliferation of industry, government or other certificate policies for its public certificates as it sees appropriate.

### **Critical Extensions**

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

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

### **Incorporation by Reference**

The GlobalSign CPS as well as other relevant 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. Information, including documents, incorporated by reference are subject of a separate statement on it.

GlobalSign reserves its right to limit certain disclosures it makes including statements on 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 addressed in a subscriber certificate. They can also be partially defined in a subscriber certificate. The remainder can be a document made available on demand 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 deemed included in the Certificate Policy extension that GlobalSign may use.



### **Certificate Policy**

GlobalSign also makes available 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.

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

### **Object Identifiers**

As a Certificate Policy Authority, GlobalSign may assign to this CPS and other applicable GlobalSign Certificate Policies an object identifier (OID). Such OID 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.

### **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 in three-hour its certificate status information resources including:

- Certificate Revocation List (CRL);
- Online Certificate Status Protocol (OCSP).

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.

### **Standards used for GlobalSign Directories**

To construct 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.

### **Standards Used for GlobalSign Certificate Requests**

To construct certificate requests GlobalSign uses standards that include:

- PKCS#10
- Microsoft IE



- Netscape certificate request
- Nokia/WTLS.

### **Subscriber Identification**

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

### **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 under the circumstances.

### **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.

### **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.

### **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.

### **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.



### **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.

### **GlobalSign Key Generation Controls**

The generation of the private key of GlobalSign requires the control of more than one appropriately authorised member of staff serving in a trustworthy position. More than one member of the management makes authorisation of key generation in writing.

### **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.

### **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 authorises key storage and assigns personnel in writing.

### **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.

### **Secret Sharing**

GlobalSign's secret shares are held by multiple authorised holders to safeguard and improve the trustworthiness of private key(s) and provide for key recovery.

### **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.

### **GlobalSign Private Key Distribution**

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



### **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 on which the keys are stored.

The key destruction process is documented and associated records are archived.



## 5. Organisation

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

### 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.

### Organisational Good Standing

GlobalSign makes reasonable efforts to meet the requirements

- Of organisations and authorities whose rules and regulations might materially affect GlobalSign's trustworthiness
- Of accreditation or licensing schemes as they may be required or associated with the delivery of GlobalSign's services.
- Set out by law or contract with regard to the provision of trust services.

While GlobalSign is an organisation that is annually audited for its financial stability the results of any such audits remain confidential.

### Compromise and Disaster Recovery

GlobalSign retains and implements a Business Continuity Plan to restore business operations in a timely manner following interruption to, or failure of critical business processes.

In a separate Business Continuity Plan, GlobalSign lists the applicable incident compromise reporting and handling procedures. The GlobalSign Business Continuity Plan address the following areas:

- Procedures to be used if computing resources, software, and/or data are corrupted or suspected to be corrupted.
- How a secure environment is re-established.
- Which certificates are revoked.
- Whether the entity key is revoked.
- How the new entity public key is provided to the users.
- How the subjects are re-certified.
- The recovery procedures used if the entity key is compromised.
- How a secure environment is re-established
- How the new entity public key is provided to the users.
- How the subjects are re-certified.
- Specific aspects on natural or other disaster.
- Availability of a remote hot-site at which operations may be recovered.
- Procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established either at the original site or at a remote site.



### **Trustworthy Systems**

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

### **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.

### **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 supported by means of an independent audit report, a self-declaration or agreement.

### **GlobalSign Accreditation**

GlobalSign may choose to comply with requirements set out by CA accreditation schemes, as they become available. The choice of the accreditation scheme to adhere to, the timing and the conditions to meet the requirements remain at the discretion of GlobalSign.

### **Financial Resources**

GlobalSign retains sufficient financial resources to maintain operations and perform duties. GlobalSign takes steps to remain reasonably able to bear risk from potential liability to subscribers and recipients of certificates as well as any other parties that may rely on information included in the certificates that have been issued. Such potential liability, however, is limited within the boundaries of the GlobalSign Limited Warranty Plan as explained below in this CPS.

### **Limited warranties**

GlobalSign makes available a limited warranty policy for selected types of its products or services to cover against commonly identified risks of digital certification. GlobalSign maintains an insurance plan with the support of a renowned insurance company.

### **Compliance Documentation**

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



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

### **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.

### **Records Retention**

GlobalSign retains, in a trustworthy manner, records of the GlobalSign digital certificates it issues. There are term periods for the retention of records. The first applies to certificates with nil transaction value (1 year). The second applies to low/medium personal transaction value certificates (5 years). The third terms applies to professional grade certificates in accordance with the requirements of the Laws of Belgium for professional records (10 years).

Records retention terms varies as follows:

- PersonalSign Demo certificates or equivalent for no less than one (1) year;
- PersonalSign 2, and PersonalSign 3 for no less than five (5) years.
- PersonalSign 2 Pro, PersonalSign 3 Pro certificates, GlobalSign Secure Server, GlobalSign Object Publishing, GlobalSign HyperSign 128, RootSign or equivalent for no less than ten (10) years;
- For public certificates, based on accreditation schemes as prescribed by such scheme.

Filing terms begin on the date of application for a GlobalSign certificate. 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 it might be required by agreement to set up a closed user group or formal requirements to comply with accreditation schemes.

### **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.

While GlobalSign makes such controls daily, audit logs are processed and archived weekly following an alarm or anomalous event, or when ever the audit log is 90% full.



Logs are kept for a period of 12 months.

For the protection of audit logs GlobalSign takes the following steps:

Audit logs can only be viewed by authorised personnel including the Security Officer. While logs are protected only the Security Officer may delete the audit file as part of rotating the audit file. Physical and logical measures are implemented to protect against deletion of audit logs.

GlobalSign implements audit log back up procedures.

The audit log accumulation system is internal to GlobalSign.

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

GlobalSign performs vulnerability assessments from time to time.

### **Logs for Core Functions**

GlobalSign maintains, in a trustworthy manner, and for a period of maximum five years logs of the following events:

- Key generation.
- Key management.
- Interruption of service.
- Perimeter controls.
- Control documentation.

### **Accessing Logs for Core Functions**

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

### **Protection of Logs for Core Functions**

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

### **Audit for Core Functions**

GlobalSign seeks audit services from specialised independent auditors for selected operations as it sees fit or as mandated by accreditation schemes. Audits organised as prescribed by accreditation schemes address subject areas as prescribed by such schemes. Audits take place e.g. annually or as otherwise prescribed by such schemes.

Audit topics may cover areas that include the following:

- CA business practices and disclosure
- Service integrity
- CA environmental controls

GlobalSign takes steps to act in coherence with audit requirements,



### **Availability of GlobalSign Certificates**

To verify a signature that is verifiable with reference to a digital certificate GlobalSign makes available to third parties copies of its own certificates as well as any related revocation data.

### **Publication**

GlobalSign publishes information in its Repository, the CRL and the GlobalSign web site. Updated versions are marked as appropriate.

### **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.

### **Accessing Information Published**

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

Proprietary, confidential or otherwise protected information is may be disclosed upon request. GlobalSign shall use its discretion on whether to disclose such information or not.

### **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, as applicable:

- 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 explicit assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.



### **Secure Facilities**

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

### **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.

### **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 or accreditation schemes.

### **Personnel Management and Practices**

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

### **Trusted Positions**

GlobalSign personnel includes all employees, contractors, 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 to be 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 infra structure.

### **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.

### **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 Data Protection Policy.

#### **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.

#### **Senior Personnel**

GlobalSign requires management and senior personnel to possess the necessary experience and familiarity with PKI to fulfil their duties.

#### **Conflicting Interests**

GlobalSign takes material steps to ensure that its members of personnel especially those in Trusted Roles do not have any conflicting roles or conflicts of interest with GlobalSign.

#### **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.

#### **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](mailto:support@globalsign.net), [legal@globalsign.net](mailto:legal@globalsign.net)
- by post, GlobalSign NV, Support, Philipssite 5, B-3001 Leuven, 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.*

### **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 completed 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.

### **Delegation**

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

### **Key Pair Generation**

Subscribers are exclusively responsible for the secure generation of their own private key pair, using a trustworthy system as required by the product or application.

### **Key Pair Protection**

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

### **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.

### **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.

### **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 the information collected from applicants of GlobalSign certificates in order to meet requirements of its own, set by the business, application or legal contexts. Such documentation includes identification elements such as the following.



### **Information Collected from Individual Applicants**

Information required to support an application for a GlobalSign certificate is listed below. GlobalSign may modify such information collected as it 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).

### **Information Collected from Legal Persons**

Information required to support an application for a GlobalSign certificate is listed below. GlobalSign may modify such information collected as it sees appropriate, in the business context of the certificate, or as it may be prescribed by law:

- 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

### **Requirements to Validate Certificate Applications**

Upon receipt of an application for a digital certificate and based on the submitted information, GlobalSign validates 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.

#### **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. However, it reserves its right to modify such registration requirements as it sees appropriate or it may be prescribed by law.

#### **Third-Party Confirmation of Business Entity Information**

GlobalSign may request third parties to confirm information concerning 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 particular 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.

#### **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 to distinguish subscribers within its own domain. GlobalSign may use the Domain Name Service for resolving RDN assignment if necessary.

#### **Time to Confirm Submitted Data**

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

#### **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 re-apply.

### **Certificate Issuance and Subscriber Consent**

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

### **GlobalSign Representations Upon Certificate Issuance**

GlobalSign makes certain representations to subscribers and relying parties. These are described in the sections below.

#### **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.

#### **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 below in this CPS. GlobalSign also extends to relying parties a conditional insurance program for certain types of damages as described below in this CPS.



### **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.

### **Certificate Validity**

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

### **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.

### **Representations by Subscriber Upon Acceptance**

By 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, uses a trustworthy system, and takes 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.

### **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 may also publish their GlobalSign certificates in repositories.

### **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 cases 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 be able to verify 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 Electronic Data Interchange (EDI), digital signatures are classified as specified security services with defined semantics. GlobalSign may support signature policies for the validation of electronic signatures 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.

### **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 considers that it has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository.

### **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.

### **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 subject's certificate.
- 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.



### **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.

### **Certificate Renewal**

Requirements for renewal are largely similar to those originally required for subscribing to the service.

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

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

The remainder of the procedures follow the initial registration process including:

- Notification of the new certificate to the subscriber;
- Procedure 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.



## **7. Legal Conditions of Issuance**

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

### **Representations of GlobalSign**

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

### **Public Services Only**

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

### **Information Incorporated by Reference in a Digital Certificate**

GlobalSign incorporates by reference the following information in the 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.

### **Pointers to Incorporate by Reference**

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

### **GlobalSign policy revision procedure**

#### **Objective**

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

#### **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.

#### **Policy updates**

GlobalSign management and/or consultants contributing to the content of the GlobalSign CP/CPS propose updates of the policies.



### **GlobalSign Policy Management Authority**

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

- At least 3 management members
- At least 2 middle management/consultants directly involved in the drafting of GlobalSign policies.

All members of the GlobalSign Policy Management Authority have one vote. No other party has any other voting right.

### **Acceptance of Updated Versions of the CPS**

Upon approval of a CPS update by the GlobalSign Policy Management Authority that CPS is published in the GlobalSign online Repository at <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 the notice. After such period the updated version of the CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the GlobalSign CPS.

### **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.

### **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.

### **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 relevant changes.



### **Interference with a GlobalSign Implementation**

Subscribers, relying parties and any other parties must 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.

### **Compliance with Software Standards**

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

### **Root Signing Partnerships**

Root Signing requires the issuance of a Root-Sign certificate to the applicant CA as described in the procedure the sections below.

#### **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 must refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities without GlobalSign's written permit.

#### **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 a partner to the extent that the service or product is not covered by the GlobalSign insurance policy featured below in this CPS. The liability for the service or product remains exclusively with the partner making the service or product available, i.e. the GlobalSign partner and not with GlobalSign.

#### **Root Sign Limitation of Liability**

As the GlobalSign network may include CAs that have been root signed by GlobalSign, GlobalSign offers limited warranty for the integrity of a 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 a partner root. The liability for a link remains exclusively with the issuer of the certificate, i.e., the GlobalSign partner and not with GlobalSign.



## **Renewal**

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

## **Secret Shares**

GlobalSign issues and uses secret shares to protect its private key.

### **Safeguarding Secret Shares**

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).

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.

### **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.

### **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.

### **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.



### **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.

### **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 service, such as OCSP, published by GlobalSign. This is because an unverified digital signature cannot be assigned as the signature of a subscriber.

Relying on a non-verifiable digital signature may result in risks with the relying party, but not GlobalSign, assume completely.

### **Refusal to Issue a Certificate**

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

### **Public Keys of Refused Applications**

Applicants for certificates that have not resulted in a 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.

### **Subscriber Obligations**

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

- Having knowledge of and if necessary seek any training on the using of digital certificates and PKI.
- Generating securely their private key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with GlobalSign including certificate application.
- 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 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 or of any fact that affects the integrity of the private key.
- Ceasing the use of a GlobalSign certificate if any featured information becomes invalid.
- Ceasing the use of a GlobalSign certificate when it becomes invalid.



- When invalid, removing 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 and taking measures for the protection of the private key.
- Complying with any restrictions in the usage of the key or certificates.
- Using secure devices and products that provide appropriate protection to their keys.
- For any acts and omissions of subscribers' partners and agents that the 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.
- 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 notifying GlobalSign of any misrepresentation and omission made by an agent.

### **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 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.**

### **Relying Party Obligations**

**A party relying on a GlobalSign certificate promises to:**

- **Have knowledge on using digital certificates and PKI.**



- Accept notice of the GlobalSign CPS and associated conditions for relying parties that GlobalSign communicates.
- Verify a GlobalSign certificate by using GlobalSign directories, e.g. 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.

### **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.

### **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 in any way 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.

### **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.

### **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.



### **GlobalSign CA Obligations**

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

- Comply with this CPS and its amendments as published under [www.globalsign.net/repository](http://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 CPS 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 CPS.
- 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 issued according to this CPS upon receipt of a valid request to revoke a certificate from a person authorised to request revocation.
- Provide support to subscribers and relying parties as described in this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Publish CRLs on a regular basis in accordance with this CPS.
- Notify relying parties of certificate revocation through published CRLs on the GlobalSign repository.
- Make a copy of this CPS and applicable policies available upon request.

**GlobalSign acknowledges it has no further obligations under this CPS.**

### **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 and authenticity actions prescribed by the GlobalSign procedures and this CPS.
- 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 CPS.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CPS.



### **GlobalSign Repository Obligations**

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

- Publish accepted certificates, revoked or suspended certificates in accordance with this CPS.

### **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.

### **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, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on 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.

### **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.

### **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.

### **Fitness for a Particular Purpose**

GlobalSign disclaims any warranty of fitness for a particular purpose.



### **Liability Caps**

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

### **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.

### **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 nuclear facilities, aircraft navigation or communication systems, air traffic control systems, weapons control systems etc. where failure could result in death, injury, or environmental damage.

### **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.

### **Compliance with Applicable Laws**

GlobalSign complies with applicable laws in Belgium.

### **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 as pertaining in Belgium.

### **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.

### **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 will indemnify without limitation GlobalSign for any loss or damage resulting from any such infringement.**

### **Intellectual Property Licensing**

Certificates are and remain property 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 accessible repository or directory without the express written permission of GlobalSign. The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.

### **Successors and Assigns**

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

### **Severability**

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

### **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 deems 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,  
Philipssite 5,  
3001 Leuven,  
Belgium.

### **Fees**

GlobalSign may charge subscriber fees for the use of GlobalSign products and services. GlobalSign retains its right to effect changes to such fees. For updated fee information you refer to: <http://secure.globalsign.net/phoenixng/index.cfm>



### **Survival**

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

### **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.

### **Jurisdiction**

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

### **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.

### **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.*

### 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.

### 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	Commission pour la Protection de la Vie Privée	Commission for the protection of Personal Data
Regentschapstraat 61 1000 Brussel Belgie Voice: +32 2 5427200 Fax: +32 2 5427212	rue de la Régence, 61 1000 Bruxelles Belgique	r. de la Régence 61 1000 Brussels, Belgium

### 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.

### 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.



## **GlobalSign representations**

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

### **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](http://www.globalsign.net/repository).

### **Only PKI Services**

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

### **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.

### **Proportionality**

GlobalSign may only request the e-mail address and the name of an applicant or subscriber. 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.

### **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. GlobalSign maintains no paper records of the credit card records, while all relevant digital information is stored off-line.

### **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.

### **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.

### **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.

**Personally Submitted Data**

GlobalSign only collects data directly from an applicant or subscriber or a duly authorised agent.

**Legal Disclosures of Personal Data**

GlobalSign only discloses personal data as required by law. In advance of such disclosures, GlobalSign informs the applicant or subscriber of the requirement to effect such disclosures to the extent permitted by law or court order.

**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.

**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).

**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.

**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.

**Cookie Policy**

GlobalSign might use non-intrusive cookie techniques to measure access to and guide users of its web site and services.

**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.

**Visitors**

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

**Links**

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

**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.

**Advertisement**

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

**Property**

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

**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.

**EU Level Privacy Protection**

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.

**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.

**Additional Personal Information**

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

**Scope of Collection of Personal Data**

GlobalSign requests only personal data that is necessary to deliver a PKI related service.

**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.

**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.

**Consent Upon Submission**

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

**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 so notified are encouraged to opt out appropriately on their registration form for GlobalSign services or products.

**Administrative and Security Announcements**

GlobalSign may use subscriber provided contact information to notify subscribers on administrative or security matters regarding GlobalSign products or services.

**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.

**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.

**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.

**Personal Data Processing Systems**

GlobalSign uses computer-based and manual filing systems to process personal data.

**Processing and Transmission Equipment**

GlobalSign uses equipment and applies appropriate procedures to transmit and store personal data.

**Auditing Procedures**

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

**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 web site.

#### **Statistical and Other Processing of Personal Data**

GlobalSign reserves its right to perform statistical, historical or scientific processing of the personal data it collects.

#### **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.

#### **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 web 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.

#### **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.

#### **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.

#### **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.

**General Information Available**

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

**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.*

### **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.

### **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.

### **Equitable Approach**

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

### **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 require 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 become aware 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.

### **Assurances of GlobalSign**

When issuing a certificate GlobalSign assures subscribers as follows:

#### **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.

#### **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.

#### **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 web site at [www.globalsign.net](http://www.globalsign.net).

#### **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 web site at: [www.globalsign.net/repository](http://www.globalsign.net/repository).

#### **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](http://www.globalsign.net) while it makes available a helpdesk service for its subscribers.

#### **Forms of Publishing**

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

#### **Multi-lingual Presentation**

GlobalSign through its extensive network of national alliance partnerships supports local languages to inform and provide legal notice in the countries in which it directly operates.

**No Spamming**

GlobalSign exclusively uses acceptable advertising methods and techniques.

**Published Identity and Product Information**

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

**Payment Information**

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

**Withdrawal Right**

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

**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.

**Contract Duration Information**

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

**Accessing Information**

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

**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.

**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.

**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 concerning the identity of the subscriber.

**General Information Available**

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

**Insurance Plan**

GlobalSign may also indicate reliance limits on the certificates it issues. For further information you may refer to *GlobalSign Limited Warranty Policy*.

**Partners**

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

**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 Limited Warranty Policy

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

### **Beneficiaries of this limited Warranty Policy and definitions**

#### **Beneficiaries**

This GlobalSign Limited Warranty 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:

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

#### **Relying Parties**

This GlobalSign Limited Warranty Policy also applies to parties relying on information featured on a GlobalSign certificate of the classes mentioned above under article 1.1.

#### **Users of PersonalSign 1 certificates**

The GlobalSign Limited Warranty Policy does not apply to users of 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.

#### **Third party beneficiary rights**

This GlobalSign Limited Warranty 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 Limited Warranty Policy Statement.

#### **Unauthorised Products**

The GlobalSign Limited Warranty Policy 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 Limited Warranty Policy to parties that make use of unauthorised products that might bear the name GlobalSign.

**Closed User Group**

This GlobalSign Limited Warranty Policy does not apply to users of products or services purchased or otherwise made available for usage within a closed user group, which will be subjected to a separate agreement unless otherwise stated in the closed user group agreement.

**GlobalSign employees, associates and administrators**

This GlobalSign Limited Warranty 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.

**Scope of Coverage****Civil liability protection**

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

**Errors in identification**

This GlobalSign Limited Warranty 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.

**Loss of documents**

This GlobalSign Limited Warranty Plan covers the risk of loss of documents related to the identification process that an applicant may submit to GlobalSign to establish their identity.

**Intentional or accidental errors:**

This GlobalSign Limited Warranty 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.

**Limited Warranty**

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

**Exceptions**



The following is a list of categories of exceptions to liability accepted by GlobalSign for a refunding of a beneficiary for any loss suffered. This list is indicative and it includes but is not be limited to the cases following below in this article.

**Honorary rewards etc.:**

Claims related to disputes from honorary rewards, costs or commercial debts.

**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 Limited Warranty Policy Statement.

**Civil liability burdens**

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

**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.

**Insolvency**

Claims as a result of the insolvency of a beneficiary are excluded from this limited Warranty policy statement. It is not intended to offer coverage to other beneficiaries.

**Control over a beneficiary**

Claims imposed by any legal entity that has control over a beneficiary, any affiliate of a beneficiary, any legal entity controlled by a beneficiary or its affiliates.

**Collective liability**

If any of the beneficiaries that are deemed responsible for the circumstances leading to a liability claim is found in one of the exception categories explained above, the exception will be extended to the rest of the beneficiaries also.

**Request for revocation**

Failure or unreasonable delay by the beneficiaries to properly dispatch a request for revocation of a GlobalSign certificate is deemed to result in the cancellation of this GlobalSign Limited Warranty Policy Statement.

**Due diligence**

Failure of the beneficiaries to exercise due diligence to prevent compromise or loss of the subscriber's private key results in the cancellation of this GlobalSign Limited Warranty Policy Statement.

**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 Limited Warranty Policy Statement.

**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 Limited Warranty Policy Statement.

**Reasonable security measures**

It results in cancelling any rights emanating from this GlobalSign Limited Warranty Policy Statement 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. The above limitations also include 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 Limited Warranty Policy Statement.

**Illegal acts**

Illegal acts by the beneficiaries being either a subscriber or a relying party result in cancelling this GlobalSign Limited Warranty 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 Limited Warranty Policy Statement. GlobalSign may appropriately seek compensation for any damages suffered as a result of illegal acts of the beneficiary.

**Misuse of services**

Any person causing damages or misusing the Internet, telecommunication or Value Added Services (VAN) including usage or reproduction of computer viruses has no right to make a rightful claim from this GlobalSign Limited Warranty Policy Statement. The above also include persons directly or indirectly engaging in reverse engineering, attacking or otherwise interfering with the technical implementation of any of the GlobalSign services. The foregoing results in the cancellation of this GlobalSign Limited Warranty Policy Statement unless permitted in writing by GlobalSign.

**Reasonable failure of equipment**

Reasonable failure of GlobalSign infrastructure or equipment does not result in the cancellation of this GlobalSign Limited Warranty 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 Limited Warranty Policy Statement.

#### **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.

#### **Sensitive equipment**

All GlobalSign non-attribute certificates provided through its public certification services, are issued for general commercial usage. This GlobalSign Limited Warranty 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.

#### **Prior authorisation**

This GlobalSign Limited Warranty 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.

#### **Limits**

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

#### **Punitive damages**

Punitive damages are excluded from this limited warranty policy statement.

#### **Field of coverage**

##### **Truthful facts**

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

##### **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.

##### **Other claims**

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

**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 Limited Warranty Policy Statement with GlobalSign makes void all claims for a refund under this limited Warranty plan.

**Temporal validity of the coverage****General**

GlobalSign shall have no obligation to make a payment unless the beneficiary submits a payment request as described below.

**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.

**Limited Warranty period**

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

**Extension of the limited Warranty period**

This GlobalSign limited Warranty 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.

**Facts**

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

**Payment Requests****Incidental or consequential damages**

The GlobalSign Limited Warranty Plan will cover any incidental or consequential damages caused by a breach of the conditions set out in this Policy and within the limits specified herein.

**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 any 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 limited Warranty 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 in appropriately informing GlobalSign about the damages, deviations from the prescribe procedures, failure to subrogate claims to.

## **Limitations on Payments for Subscribers**

### **Maximum limits**

The GlobalSign Limited Warranty 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 Limited Warranty Plan for Subscribers**

PersonalSign 2 Certificates	2500 EURO
PersonalSign 2 Pro Certificates	2500 EURO
PersonalSign 3 Certificates	37500 EURO
PersonalSign 3 Pro Certificates	37500 EURO
ServerSign Certificates	37500 EURO
ObjectSign Certificates	37500 EURO
HyperSign 128 Certificates	37500 EURO
ServerSign for WAP Certificates	37500 EURO

### **Apportionment of claims**

Damages exceeding the liability cap set for any given certificate shall be apportioned first to the earliest claims to achieve final resolution unless otherwise provided by a court of competent jurisdiction.

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.

## **Limitations on Payments for Relying Parties**

### **Maximum limitations for relying parties**

The GlobalSign Limited Warranty Plan sets limits to the maximum amount GlobalSign may pay to a 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 of a certificate to the limits per category as set for subscribers, i.e. a maximum of 2500 EURO per GlobalSign class 2 certificates and 37500 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 Limited Warranty Plan for Relying Parties**

PersonalSign 2 Certificates	2500 EURO
PersonalSign 2 Pro Certificates	2500 EURO
PersonalSign 3 Certificates	37500 EURO
PersonalSign 3 Pro Certificates	37500 EURO
ServerSign Certificates	37500 EURO
ObjectSign Certificates	37500 EURO
HyperSign 128 Certificates	37500 EURO
ServerSign for WAP Certificates	37500 EURO

### **Limitation on Payment for Subscribers and Relying Parties**

#### **Liability caps**

The liability caps provided under articles above will remain as stated regardless of the number of digital signatures, transactions, or claims related to a certificate.

### **Maximum Limits**

#### **General**

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

#### **Maximum limits**

The maximum limit is the amount that GlobalSign may refund a beneficiary with (a subscriber or a relying party) for a breach of a limited Warranty in the limited Warranty period.

Payments made by GlobalSign may ultimately reduce the amount available for future payments.

#### **Total amount for limited Warranty exhausted**

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

#### **New certificates**

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



### **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.

### **Single transaction**

If a subscriber makes usage of multiple certificates for the same transaction he may indicate, following an appropriate declaration by the means of art. 6.2, which certificates provide the limited Warranty for this transaction.

### **Updates and Amendments**

This GlobalSign Limited Warranty 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. It is the beneficiary's responsibility to monitor changes and obtain the latest version of this and other agreements and policy statements that apply in the provision of the service.

### **Force Majeure**

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

### **Conflict of Provisions**

In case of conflict between this GlobalSign Limited Warranty Policy Statement and the CPS, the CPS shall prevail.

### **Severability**

If any provision of this GlobalSign Limited Warranty 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 Limited Warranty Policy Statement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so that it reasonably effects the intent of its parties.

Provisions of this GlobalSign Limited Warranty 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.

### **Governing law**

This GlobalSign Limited Warranty Policy Statement is governed by the Law of Belgium. The Courts of Brussels have exclusive jurisdiction over any dispute related to this Limited Warranty Plan.

**Statutory rights**

This GlobalSign Limited Warranty 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.*

### Personal Certificates

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

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

### Server Certificates

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

- **ServerSign™**: ServerSignis meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in commercial and financial transactions. The identity of the ServerSign-holder is fully-authenticated by GlobalSign.
- **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.

### **Object Publishing Certificates**

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

- **ObjectSign™** ensures the identity of an entity that distributes software 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.

### **Acceptable Subscriber Names**

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

### **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.

### **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, Philipssite 5, 3001 Leuven, Belgium, Attn. Legal Practices or [legal@globalsign.net](mailto:legal@globalsign.net).



## 12. PersonalSign 1 Demo

*This part describes the specific requirements for PersonalSign 1 certificates.*

### 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 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 demo certificates are intended for test purposes only.

PersonalSign 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 demo certificates are free of charge.

PersonalSign 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.

### 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.**

### Individuals

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



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

**E-mail (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 the information to be included in the certificate.

## Content

Typical of information published in 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 of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

## Certificate Profile

PersonalSign Demo	
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
CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

### **Submitted documents to identify the applicant**

No documents are required for PersonalSign Demo certificates.

### **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 Demo verification might require 1 working day.

### **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 from which 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 an on line database.
- 10 Renewal: not allowed
- 11 Revocation: allowed but remains at GlobalSign's discretion

### **Limited Warranty**

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

### **Relevant GlobalSign Legal Documents**

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

#### General

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

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

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 undertaken by a registration authority by using a copy of an identity proof.

PersonalSign 2 certificates are issued primarily for personal communications and usages. No transaction value communications or usage can be done with a PersonalSign 2 certificate for intra -organisational and inter-organisational E - mail; small, "low-risk" transactions; personal/individual E-mail; password replacement; software validation; online purchases and on-line subscription services.

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

#### 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.**

#### Individuals:

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

**On-line:** Via the Web (<https>). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign.

Additional documentation in support of the application may be required so



that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of the information to be included in the certificate.

**E-mail (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 the information to be included in the certificate.

## Content

Typical 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

## Certificate Profile

PersonalSign 2 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	Not Critical / 0xA0
BASIC CONSTRAINT	NO



CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

### **Documents Submitted to Identify the Applicant**

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

### **Time to Confirm Submitted Data**

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

### **Issuing Procedure**

The following steps describe the milestones in the procedure 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 on line database.
- 12 Renewal: allowed.
- 13 Revocation: allowed.

### **Limited Warranty**

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



### **Relevant GlobalSign Legal Documents**

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

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



## 14. PersonalSign 2 Pro

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

### General

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

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

GlobalSign uses encryption software protected by a Personal Identification Number (PIN) to issue PersonalSign 2.

PersonalSign 2 Pro certificates validity period is 1 year.

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

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

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

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

### Individuals

A certificate request can be made by the following means:

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

**E-mail (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 information to be included in the certificate.

## Content

Typical content of information published on a PersonalSign 2 Pro 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

## 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	Not Critical / 0xA0
BASIC CONSTRAINT	NO
CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

## Documents Submitted to Identify the Applicant

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



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

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

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

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

### **Time to Confirm Submitted Data**

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

### **Issuing Procedure**

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

- 1 The applicant fills out the online request on GlobalSign's website
- 2 The applicant submits the required information, i.e. 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 Applicant must mail to an LRA copies of identity, articles of association, professional context and payment information.
- 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.

### **Limited Warranty**

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



### **Relevant GlobalSign Legal Documents**

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

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



## 15. PersonalSign 3

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

### General

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

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

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

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

PersonalSign 3 certificates validity period is 1 year.

PersonalSign 3 certificates are issued primarily for **personal communications** and usages. No value communications or usages are prescribed for PersonalSign 3 certificate for intra -organisational and inter-organisational E-mail.

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

### Individuals:

A certificate request can be made as follows:

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

**E-mail (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 information to be included in the certificate.

### 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

### Certificate Profile

PersonalSign 3 Profile	
CN	GlobalSign Class 3 CA
O	GlobalSign NV/SA
OU	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
CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

### 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 a copy of identity proof.

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



### **Time to Confirm Submitted Data**

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

### **Issuing Procedure**

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

- 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 in which 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. **NB. Personal presence may occur prior to the time of the application**
- 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.

### **Limited Warranty**

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

### **Relevant GlobalSign Legal Documents**

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

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



## 16. PersonalSign 3 Pro

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

### 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 Pro certificates validity period is 1 year.

PersonalSign 3 certificates are issued primarily for professional usages.

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

### Individuals

A certificate request can be made as follows:

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

**E-mail (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 information to be included in the certificate.

## Content

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

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

## Certificate Profile

<b>PersonalSign 3 Pro Profile</b>	
CN	GlobalSign Class 3 CA
O	GlobalSign NV/SA
OU	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
CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

## 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 membership card is required in addition to the above -mentioned documents.

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

### **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.

### **Issuing Procedure**

The following steps describe the milestones in the issuance of a PersonalSign 3 Pro 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 with which 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. **NB. Personal presence may occur prior to the time of the application.**
- 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.

### **Limited Warranty**

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



### **Relevant GlobalSign Legal Documents**

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

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



## 17. ServerSign

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

### 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.

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

### Business Entities

A certificate request can be made in the following ways:

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

**E-mail (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 information to be included in the certificate.

### Content

Typical information published on a ServerSign certificate includes the following elements

- Applicant's domain name



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

### Certificate Profile

ServerSign Profile	
CN	GlobalSign Secure Server CA
O	GlobalSign NV/SA
OU	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
CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

### 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.

### 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.

### Issuing Procedure

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



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

### **Limited Warranty**

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

### **Relevant Globalsign Legal Documents**

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

- 1 CPS
- 2 Subscriber Agreement
- 3 Limited WarrantyPolicy



## 18. ObjectSign

*This part describes the specific requirements for ObjectSign certificates.*

### General

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

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.

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

### Business Entities

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

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

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

### Content

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

- Applicant's e-mail address
- Applicant's name of organisation
- Applicant's public key
- Code of applicant's country



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

### 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
CERTIFICATE POLICIES	NO
SIGNATURE ALGORITHMS	md5/RSA

### 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).

### Time to Confirm Submitted Data

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

### Issuing Procedure

Below following the steps 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 at which 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 an online database
- 12 Renewal: allowed
- 13 Revocation: allowed

### **Limited Warranty**

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

### **Relevant GlobalSign Legal Documents**

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

- 1 CPS
- 2 Subscriber Agreement
- 3 Limited WarrantyPolicy
- 4 Data Protection Policy (if applicable)

### **GlobalSign Private Key Protection**

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

### **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.

### **Possible Applications Supported**

The examples listed 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.



## 19. HyperSign 128

*This part describes the specific requirements for HyperSign 128 certificates.*

### General

HyperSign 128 certificates are meant for secure communication with a web site through an SSL link that allows for 128-bit encryption.

HyperSign 128 certificates provide a high level of credibility for an organisational web site.

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

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](http://www.globalsign.net/repository).

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

### Business Entities

A certificate request can be made as follows:

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

**E-mail (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 on information to be included in the certificate.



## **Content**

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

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

## **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.

## **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.

## **Issuing Procedure**

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

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

**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.

**Limited Warranty**

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

**Relevant GlobalSign Legal Documents**

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

- 1 CPS
- 2 Subscriber Agreement
- 3 Limited WarrantyPolicy

**Documentation**

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

**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.

**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.



## 20. ServerSign for WAP

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

### 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.

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

### 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

### 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.

### 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.

### Issuing procedure

Hereunder follow the steps of the registration procedure for a ServerSign for WAP certificate:



- 1 Applicant creates a Certificate Signing Request (CSR).
- 2 Applicant follows the 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 is 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 through third party databases or resources
- 7 GlobalSign may positively verify the applicant.
- 8 GlobalSign publishes the issued certificate in online database.
- 9 Renewal: allowed.
- 10: Revocation: not allowed.

### **Limited Warranty**

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

### **Relevant GlobalSign Legal Documents**

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

- 1 CPS
- 2 Subscriber Agreement
- 3 Limited WarrantyPolicy



## 21. Root-sign certificates

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

### General

Root-sign certificates are CA certificates. Root-sign 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.

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

### Business Entities

A certificate request can be made in the following manner:

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

### Content

Typical 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



### **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 applicant organisation.

### **Time to Confirm Submitted Data**

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

### **Issuing Procedure**

The following steps describe the milestones in the process of 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 is 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 its 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

### **Limited Warranty**

GlobalSign extends a conditional insurance plan to selected Root-signed CAs with which it has validly entered into a Root-sign agreement. 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.

### **Relevant Globalsign Legal Documents**

The applicant must take notice of and is bound by the following documents available on [www.globalsign.net/repository](http://www.globalsign.net/repository):

- 1 CPS
- 2 GlobalSign Root-sign agreement.



## 22. 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 from a relying party.

### **AUTHENTICATION**

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

### **AUTHORISATION**

Granting of rights.

### **AVAILABILITY**

The rate of accessibility of information or resources.

### **BINDING STATEMENT**

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 be consulted by relying parties at all times prior to relying on information featured in a certificate.

### **CERTIFICATE SERIAL NUMBER**

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

### **CERTIFICATE SIGNING REQUEST (CSR)**

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

### **CERTIFICATION**

The process to issue a digital certificate.

### **CERTIFICATION AUTHORITY (CA)**

An authority, such as 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 connects 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 is submitted to the relevant CA during the 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**

Documents describing GlobalSign's internal security and/or registration 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 an RA (See, Registration Authority) to perform the registration of applications and related data for digital certificates. An LRA 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 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.

**ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)**

A real time certificate status information resource.

**ORGANISATIONAL CERTIFICATES**

Digital certificates where an organisation is named on the subject line.

**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.

**REGISTRATION AUTHORITY**

An entity (organisation) appointed by a CA to perform the registration and approval applications for digital certificates. An 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. An RA may appoint an LRA (See, Local Registration Authority) to perform the function of data registration for digital certificates.

**RELYING PARTY**

A recipient who acts by relying 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**

A 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.

**SIGNATURE POLICY**

Set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid

**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**

To temporarily make a digital certificate inoperable.

**TIME STAMP**

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 of 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**

Philipssite 5  
B-3001 Leuven, Belgium

URL: <http://www.globalsign.net>  
E-mail: [info@globalsign.net](mailto: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](mailto:legal@globalsign.net)

The trademarks "GlobalSign" and "BeISign" are registered trademarks of GlobalSign NV/SA.

### **Changes forecast**

This is the final version 4.1. No more changes are expected for v.4.1