GlobalSign™
GMO Internet Group

GlobalSign ExtentedSSL SUBSCRIBER AGREEMENT

This Subscriber Agreement (“Agreement”) between GlobalSign and the Applicant (“Subscriber”) identified below and signatories hereto consist of this signature page and is made effective as of the effective date specified below (“Effective Date”).

Intending to be legally bound and having reviewed this Agreement in its entirety, GlobalSign and Applicant have caused this Agreement to be executed by their authorized representatives.

<FULL LEGAL NAME OF GLOBALSIGN>
(“GlobalSign”)
Address: ______

Reg. N°/Tax ID: ______

AND

<FULL LEGAL NAME OF APPLICANT>
(“Subscriber”)
Address: ______

Reg. N°/Tax ID: ______

Agreed for and on behalf of GlobalSign:
Name : ______
Title : ______
Date : ______

Signature : ______

Agreed for and on behalf of Subscriber:
Name : ______
Title : Contract Signer
Date : ______

Signature : ______

AGREEMENT DETAILS:
Effective Date: <insert date in format like 01-JAN-2006>

IT IS AGREED AS FOLLOWS:

The parties acknowledge that the present subscriber agreement applies to the GlobalSign ExtentedSSL digital certificate to be issued pursuant to the provisions set forth in the GlobalSign Certification Practice Statement (CPS) which incorporates by reference the CA/Browser Forum Guidelines for Extended Validation Certificates.

The parties therefore acknowledge that the CA/Browser Forum Guidelines for Extended Validation Certificates set forth mandatory requirements as to issuance and management of GlobalSign ExtentedSSL certificates.

GlobalSign CPS is incorporated by reference hereto and is available at www.globalsign.com. The CA/Browser Forum Guidelines for Extended Validation Certificates are available at www.cabforum.org.

The parties shall ensure that the present subscriber agreement is properly signed before requesting the issuance of the GlobalSign ExtentedSSL digital certificate.

1. Authority to Use Digital Certificates

Grant of Authority

As to the Effective Date, GlobalSign hereby grants to the subscriber the authority for the term set forth in Sections 6 and 7 to use the requested GlobalSign ExtentedSSL Certificate in conjunction with private key or public key operations.

Limitations on Authority

The subscriber shall use the requested GlobalSign ExtentedSSL Certificate only in connection with properly licensed cryptographic software. Digital Certificate can only be installed on licensed number of physical server as specified during enrolment.

2. Services Provided by GlobalSign

After execution of this agreement and payment of all applicable fees, in addition to the grant of authority pursuant of Section 2, GlobalSign or a third party provider designated by GlobalSign shall provide the following services to the subscriber:

CRL Availability

GlobalSign shall use reasonable efforts to compile, aggregate and make electronically available to all CA's and certified users in the Secure Server Hierarchy (i) GlobalSign current CRL and (ii) the CRLs provided by CAs to GlobalSign; provided, however that GlobalSign shall not be in breach of its obligations hereunder as a result of any delay in or failure of performance on its part which arises out of any equipment failure or telecommunications breakdown beyond the reasonable control of GlobalSign.

Revoke Digital Certificates

GlobalSign, upon the request of the subscriber, shall promptly revoke the digital certificate of the subscriber. GlobalSign agrees to it shall, promptly after revoking the subscriber's certificate at the subscriber's request, issue a new GlobalSign ExtentedSSL certificate upon data verification and validation and payment by the subscriber of the then-current applicable fee.

3. Subscriber's Obligations

Data accuracy

The subscriber undertakes to provide accurate and complete information at all times to GlobalSign, both in the GlobalSign ExtentedSSL Certificate Request and as otherwise requested by GlobalSign CA in connection with the issuance of the GlobalSign ExtentedSSL Digital Certificate(s) to be supplied by GlobalSign.

The subscriber shall also refrain from submitting to GlobalSign or any GlobalSign CA directory any material that contains statements that violate any law or the rights of any party.

Key Generation

Under the GlobalSign model the subscriber uses a trustworthy system in order to generates, its own private-public keys, in which case the following terms also apply:
(a) The subscriber generates subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures;

(b) The subscriber uses a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.

Protection of Private Key

The subscriber or a subcontractor (e.g. hosting provider) undertakes to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the private key that corresponds to the public key to be included in the requested GlobalSign ExtentedSSL certificate(s) (and any associated access information or device – e.g., password or token).

The subscriber shall ensure that the public key submitted to the GlobalSign CA correctly corresponds to the private key used.

The subscriber shall exercise appropriate and reasonable care to avoid unauthorized use of its private key.

Acceptance of GlobalSign ExtentedSSL Certificate

The subscriber shall not install and use the GlobalSign ExtentedSSLcertificate(s) until it has reviewed and verified the accuracy of the data in each GlobalSign ExtentedSSL Certificate.

Use of GlobalSign ExtentedSSL Certificate

The subscriber shall install the GlobalSign ExtentedSSL certificate only on the server accessible at the domain name listed on the GlobalSign ExtentedSSL certificate, and to use the GlobalSign ExtentedSSL certificate solely in compliance with all applicable laws, solely up to contracted server licenses, solely for authorized company business, and solely in accordance with the subscriber agreement.

Reporting and Revocation Upon Compromise

The Subscriber undertakes to promptly cease using a GlobalSign ExtentedSSL certificate and its associated private key, and promptly request the CA to revoke the GlobalSign ExtentedSSL certificate, in the event that:
(a) any information in the GlobalSign ExtentedSSL certificate is or becomes incorrect or inaccurate, or
(b) there is any actual or suspected misuse or compromise of the Subscriber's private key associated with the public key listed in the GlobalSign ExtentedSSL certificate;

Termination of Use of SureServer Certificate

The subscriber shall promptly cease all use of the Private Key corresponding to the Public Key listed in a GlobalSign ExtentedSSL certificate upon expiration or revocation of that GlobalSign ExtentedSSL certificate.

4. Permission to Publish Information

The subscriber agrees that GlobalSign may publish the serial number of the subscriber's GlobalSign ExtentedSSL certificate in connection with GlobalSign dissemination of CRL's and possible OCSP within and outside the GlobalSign Secure Server Hierarchy.

5. Disclaimer of Warranty

IN NO EVENT (EXCEPT FOR FRAUD OR WILFULL MISCONDUCT) SHALL GLOBALSIGN BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THE CPS, EXCEPT FOR

DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THE CPS) ON THE VERIFIED INFORMATION ON THE MOMENT OF ISSUANCE OF THE CERTIFICATE IN A SECURE SERVER CERTIFICATE TILL AN AMOUNT OF 2,000 $ PER SUBSCRIBER OR RELYING PARTY PER SURESERVER CERTIFICATE.
GLOBALSIGN WILL NOT BE LIABLE IN THIS CASE IF THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILFULL MISCONDUCT OF THE APPLICANT. GLOBALSIGN WILL NOT BE LIABLE IN THIS CASE IF THE USER HAS NOT RESPECTED HIS OBLIGATIONS MENTIONED IN THE CPS AND IN THIS AGREEMENT

6. Term and Termination

This agreement shall terminate at the earliest of

6.1. one or two years from the Effective Date, depending on the order of an ExtentedSSL 1 year or an ExtentedSSL 2 years.
6.2. failure by the subscriber to perform any of its material obligations under this agreement if such breach is not cured within thirty (30) days after receipt of notice thereof from GlobalSign.

7. Effect of termination

Upon termination of this agreement for any reason, the subscriber’s GlobalSign ExtentedSSL Certificate shall be revoked by GlobalSign in accordance with GlobalSign procedures then in effect. Upon revocation of the subscriber’s GlobalSign ExtentedSSL Certificate for any reason, all authority granted to the subscriber pursuant to section 2 shall terminate. Such termination shall not affect sections 4, 5, 6, 8 and 9 of this agreement which shall continue in full force and effect to the extent necessary to permit the complete fulfillment thereof.

8. Miscellaneous Provisions

Applicable Law

This Agreement shall be governed by and construed in accordance with the laws of Belgium

Binding Effect

Except as otherwise provided herein, this agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. Neither this agreement not the subscriber’s digital certificate shall be assignable by the subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit GlobalSign to terminate this agreement.

Entire Agreement

This Agreement constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties.

Notices

When the subscriber desires or is required to give any notice, demand, or request to GlobalSign with respect to this agreement, each such communication shall be in writing and shall be effective only if it is delivered by a courier service that confirms delivery in writing or mailed, certified or registered mailed, postage prepaid, return receipt requested, addressed to GlobalSign, Philipssite 5, 3001 Leuven, Belgium, Attention: Secure Server Center.
Such communications shall be effective when they are received.

Severability

Invalidity or unenforceability of one or more provisions of this Agreement shall not affect any other provision of this Agreement.

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES OR EXCLUSION OF DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

Trade names, Logos

By reason of this agreement or the performance hereof, the subscriber and GlobalSign shall acquire no rights of any kind in any trademark, brand name, logo or product designation of the other party and shall not make any use of the same for any reason except as otherwise authorized in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

9. Notice

You have to notify GlobalSign immediately if there is an error in your certificate. Without reaction from the subscriber with 15 days after receipt, the certificate is deemed accepted.

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

Definitions

Digital Certificate
A collection of electronic data consisting of a Public Key, identifying information about the owner of the Public Key, and validity information, which has been Digitally Signed by GlobalSign. Certified shall refer to the condition of having been issued a valid Digital Certificate by GlobalSign, which Digital Certificate has not been revoked.

Certificate Revocation List ("CRL")
A collection of electronic data containing information concerning revoked Digital Certificates

Certification Authority ("CA")
GlobalSign or an entity which is certified by GlobalSign to issue Digital Certificates to Users in a Digital Certificate Hierarchy GlobalSign is Customer's CA hereunder.

Digital Signature
Information encrypted with a Private Key which is appended to electronic data to identify the owner of the Private Key and verify the integrity of the electronic data. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

Private Key
A mathematical key which is kept private to the owner and which is used to create Digital Signatures or to decrypt electronic data

Public Key
A mathematical key which is available publicly and which is used to verify Digital
Signatures created with the matched Private Key and to encrypt electronic data which can only be decrypted using the matched Private Key.

Secure Server Hierarchy
A collection of CAs and their Certified Users

User
An individual or an organization that has requested a CA to issue him, her or it a Digital Certificate