



GlobalSign Subscriber Agreement for ExtendedSSL Certificates (US)

Version 1.7

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANISATION. BY USING THE DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED DIGITAL CERTIFICATE OR CANCEL THE ORDER WITHIN 7 DAYS OF ISSUANCE TO GLOBALSIGN FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@globalsign.com

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: _____

**Agreed for and on behalf of
GlobalSign:**

Name : _____
Title : _____
Date : _____

Signature : _____

**<FULL LEGAL NAME OF
APPLICANT>**

AND ("Subscriber")

Address: _____

Reg. N°/Tax
ID: _____

**Agreed for and on behalf of
Subscriber:**

Name : _____
Title : Contract Signer
Date : _____

Signature : _____

AGREEMENT DETAILS:

Effective Date: <insert date in format like 01-JAN-2008>

IT IS AGREED AS FOLLOWS:

The parties acknowledge that the present subscriber agreement applies to the GlobalSign ExtendedSSL 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 ExtendedSSL 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 ExtendedSSL digital certificate.

1. 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

Subscriber

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

2. 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 7 and 8 to use the requested GlobalSign ExtendedSSL Certificate in conjunction with private key or public key operations.

Limitations on Authority

The subscriber shall use the requested GlobalSign ExtendedSSL 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.

3. 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 will revoke an ExtendedSSL Certificate it has issued upon the occurrence of any of the following events:

- The Subscriber requests revocation of its ExtendedSSL Certificate.
- GlobalSign obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the ExtendedSSL Certificate) has been compromised, or that the ExtendedSSL Certificate has otherwise been misused;
- GlobalSign receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
- GlobalSign receives notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, etc.
- GlobalSign receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the ExtendedSSL Certificate, or that the Subscriber has failed to renew its domain name;
- GlobalSign receives notice or otherwise becomes aware of a material change in the information contained in the ExtendedSSL Certificate;
- A determination, in GlobalSign's sole discretion, that the ExtendedSSL Certificate was not issued in accordance with the terms and conditions of the Extended Validation Guidelines or GlobalSign's ExtendedSSL Policies;
- If GlobalSign determines that any of the information appearing in the ExtendedSSL Certificate is not accurate.
- GlobalSign ceases operations for any reason and has not arranged for another ExtendedSSL CA to provide revocation support for the EV Certificate;
- GlobalSign's right to issue ExtendedSSL Certificates under these Guidelines expires or is revoked or terminated [unless GlobalSign makes arrangements to continue maintaining the CRL/OCSP Repository];

- GlobalSign's Private Key for its ExtendedSSL issuing CA Certificate has been compromised;
- GlobalSign receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GlobalSign's jurisdiction of operation.
- The continued use of the certificate is harmful to the GlobalSign Trust model.

When considering whether certificate usage is harmful to GlobalSign, GlobalSign considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

Site Seal

GlobalSign permits Applicants to make use of GlobalSign's Site Seal on the Applicant's web site with a maximum daily rate of 500,000 [five-hundred-thousand] impressions per day. GlobalSign maintains the right to limit or stop the availability of the seal if this limit is exceeded.

4. Subscriber's Obligations

This subscriber agreement specifically names Microsoft as an express third-party beneficiary. As such the subscriber warrants and covenants to GlobalSign and all certificate beneficiaries the following:

Exclusive Domain Control

The subscriber acknowledges and asserts that they have exclusive control of the domain(s) for which they are applying for a GlobalSign ExtendedSSL Certificate. Should exclusive control cease for any domain(s), the subscriber acknowledges that they will promptly inform GlobalSign in accordance with the obligations of the 'Reporting and Revocation' section of this agreement.

Data accuracy

The subscriber undertakes to provide accurate and complete information at all times to GlobalSign, both in the GlobalSign ExtendedSSL Certificate Request and as otherwise requested by GlobalSign CA in connection with the issuance of the GlobalSign ExtendedSSL 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 generate, 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 ExtendedSSL 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 ExtendedSSL Certificate

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

Use of GlobalSign ExtendedSSL Certificate

The subscriber shall install the GlobalSign ExtendedSSL certificate only on the server accessible at the domain name listed on the GlobalSign ExtendedSSL certificate, and to use the GlobalSign ExtendedSSL 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

The Subscriber undertakes to promptly cease using a GlobalSign ExtendedSSL certificate and its associated private key, and promptly request GlobalSign to revoke the GlobalSign ExtendedSSL certificate, in the event that:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject.
- The Subscriber indicates that the original ExtendedSSL Certificate Request was not authorized and does not retroactively grant authorization;
- The certificate's subject or their appointed subscriber has breached a material obligation of the CPS.
- The performance of a person's obligations under the 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.
- This Subscriber Agreement has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- The information within the Certificate, other than non - verified Subscriber Information, is incorrect or has changed

Termination of Use of ExtendedSSL Certificate

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

5. Permission to Publish Information

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

6. 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 250,000 EURO PER SUBSCRIBER OR RELYING PARTY PER EXTENDEDSSL 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

7. Term and Termination

This agreement shall terminate at the earliest of

- 7.1. one or two years from the Effective Date, depending on the order of an ExtendedSSL 1 year or an ExtendedSSL 2 years.
- 7.2. 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.

8. Effect of termination

Upon termination of this agreement for any reason, the subscriber's GlobalSign ExtendedSSL Certificate shall be revoked by GlobalSign in accordance with GlobalSign procedures then in effect. Upon revocation of the subscriber's GlobalSign ExtendedSSL 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.

9. Miscellaneous Provisions

Governing Laws

This Agreement shall be governed by, construed under and interpreted in accordance with the laws of New Hampshire, US without regard to its conflict of law provisions. Venue shall be in the courts of New Hampshire.

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 nor 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

Whenever 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 mail, postage prepaid, return receipt requested, addressed to GlobalSign at one of our International offices as listed on <http://www.globalsign.com/company/contact.htm>, Attention: Legal department.

Such communications shall be effective when they are received.

Permission to utilize third party databases.

For natural persons, GlobalSign may validate items such as name, address and other personal information supplied during the application against appropriate third party databases. By accepting these terms and conditions you consent to such checks being made. In performing these checks, personal information provided by you may be disclosed to registered Credit Reference Agencies, which may keep a record of that information. You can rest assured that this is done only to confirm identity and as such a credit check is not performed. Your credit rating will not be affected by this process.

Trade Names, Logos.

By reason of this Agreement or the performance hereof, 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 authorised in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

10. NOTICE

You have to notify GlobalSign through any of our International offices as listed on <http://www.globalsign.com/company/contact.htm> immediately if there is an error in your certificate. Without reaction from the subscriber within 7 days from receipt, the certificate is deemed accepted.

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