GlobalSign EPKI Service Agreement - Version 3.0

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SERVICE. BY USING THE SERVICE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU WILL NOT BE PERMITTED TO CONTINUE AND WILL NOT BE ABLE TO ACCESS THE SERVICE. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@globalsign.com

This GlobalSign EPKI Service Agreement ("Agreement") shall become effective between GlobalSign and the organization agreeing to this Agreement ("Company") upon your acceptance of the terms and conditions stated herein by clicking the “I agree to the EPKI Service Agreement” button below (the "Effective Date").

1. Definitions

For the purposes of this Agreement, all capitalized terms used in this Agreement shall have the meaning ascribed to them in this Section 1 and elsewhere in this Agreement.

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0 and later.
Applicant: The private organization, business entity, government entity, international body or individual that applies for (or seeks renewal of) a Digital Certificate naming it as the “Subject”.
CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0 and later.
Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.
Certification Authority (CA): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. GlobalSign is the CA hereunder.
CPS: GlobalSign’s Certification Practice Statement available at http://www.globalsign.com/repository/.
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.
EPKI Administrator: Acts as the LRA in respect to identifying and authenticating Subscribers and also performs administrator tasks associated with the life cycle management of Certificates issued from the Service including renewal, revocation, re-issuance, and reporting functions.
GlobalSign: The GlobalSign entity to which Company applied for the Service, either GMO GlobalSign Limited, GMO GlobalSign, Inc., or GMO GlobalSign Pte. Ltd; GMO GlobalSign Certificate Services Pvt. Ltd or GMO GlobalSign Russia LLC.
Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. The Issuing CA may be either a Root CA or Subordinate CA.
Key Pair: The Private Key and its associated Public Key.
Local Registration Authority (LRA): The EPKI Administrator appointed (other than GlobalSign) that is responsible for identifying and authenticating Subscribers requesting Certificates. The LRA does not issue Certificates but requests the issuance of Certificates on behalf of Subscriber whose identity the LRA has verified. Under this Agreement, Company shall be the LRA.

North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) Standards – WEQ-012 v3.0 and NAESB Accreditation Requirements for Authorized Certification Authorities: The technical and management details which a Certification Authority is required to meet in order to be accredited as an Authorized Certification Authority (ACA) by NAESB.
Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party: Any natural person or legal Entity that relies on a valid Certificate.
Root CA: The top level Certification Authority whose Root Certificate is distributed by application software suppliers and that issues Subordinate CA Certificates.
Service: The EPKI service provided by GlobalSign to Company and Subscribers, a service under which Company applies for, issues, manages, and uses Certificates, and GlobalSign generates such Certificates and provides related services to Company on an out-source basis.
Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.
Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

2. Use of the Service

GlobalSign hereby grants to Company the right to use the Service under the terms set forth in this Agreement. Company shall use the Service only for purposes that are permitted by (a) this Agreement and the CPS, and (b) any applicable laws and regulations, including any laws regarding the export of data or software.

3. Services Provided by GlobalSign

GlobalSign shall operate either a shared Certificate Issuing CA or private CA to issue the Certificates upon approval of the EPKI Administrator who shall authenticate and validate the application and enrollment information of the Subscribers.
The Service is provided as a web-based service but may also be provided as an API service at Customer's option. If the Service is used in conjunction with any third party products, GlobalSign may specify certain specifications to be met by Company.

Certificates managed in conjunction with AEG shall be received and delivered through AEG acting as a proxy between the Service and Company's Active Directory.

If the Service is used in conjunction with products provided by third parties, Company may be required to comply with additional technical requirements and/or third party terms and conditions for the use of such products.

4. Optional Services or Features

4.1 Auto Enrollment Gateway (AEG)

If Company is licensing the Auto Enrollment Gateway software, use of such software shall be subject to the terms and conditions delivered with the software.

4.2 Private Hosted CA

If Company is purchasing a hosted private CA as part of the Service, Company shall complete a CA questionnaire profile that details the specifications of Company's hosted private CA.

Company acknowledges and agrees that GlobalSign owns and operates the private CA issued in the name of Company and the Issuing CA Certificate and corresponding Key Pair cannot be transferred.

4.3 Time-stamping Services for PDF

GlobalSign offers the ability to timestamp Portable Document Format (PDF) documents as a paid GlobalSign service. The number of signatures per year allowed by this service is provided during the application process. GlobalSign reserves the right to withdraw the service or charge additional fees for the service where the volume of time stamping operations performed by Company is in excess of the number purchased.

5. Company's Obligations

Company shall:

(a) Appoint an EPKI Administrator to set-up the Service including registering an organization profile, ordering EPKI license packs, and configuring the Service for a variety of settings, i.e. create email templates, and performing the registration authority duties necessary for issuance of the Certificate provided by the Service, including enrollment process for the Certificate, and be solely responsible for verifying the identity and information stipulated in the Certificate;
(b) At Company's option, appoint EPKI Administrator(s) with authority to review and optionally approve requests for Certificates and to order, manage, and revoke the Certificates provided under the Service. The EPKI Administrator may complete the enrollment process for the Applicant provided that the email address associated with the Applicant is owned and/or controlled by Company or the EPKI Administrator has explicit authorization from the Applicant to complete the enrollment process on his/her behalf;
(c) Ensure the Certificate or user name and password issued to the EPKI Administrator which enables an individual to perform the Local Registration Authority functions (collectively, the "Administrator Certificate") is secure and accessible only by the authorized individual(s);
(d) Ensure that information provided on the enrollment requests is complete and accurate;
(e) Protect the confidentiality of Private Keys from unauthorized use, access or disclosure by use of the Trustworthy System, and require the same of Subscriber;
(f) Promptly revoke or request GlobalSign to revoke the Certificate in the event of 1) the Subscriber's violation of the Subscriber Agreement, or 2) any actual or suspected loss, disclosure, or other compromise of the associated Private Key;
(g) Promptly request that GlobalSign revoke the Administrator Certificate upon 1) any change to the information on the Administrator Certificate, or 2) any actual or suspected loss, disclosure, or other compromise of the Administrator Certificate;
(h) Enters into and ensures compliance by each Subscriber with the terms of the Subscriber Agreement, either directly through the Service or through Company's own workflow process. If Company is operating a publicly trusted CA as part of the Service then the Subscriber Agreement must contain terms no less stringent than those in the GlobalSign subscriber agreement at https://www.globalsign.com/repository/;
(i) Act as the sole intermediary for all communications with Applicants and Subscribers;
(j) Create and keep records of 1) Subscriber identity verification and 2) Certificate revocation;
(k) In the case of EPKI for PDF Signing Digital Certificates for Adobe CDS or AATL, 1) ensure and enforce all Private Key generations are performed on the required cryptographic device

(as defined in the CPS) and are never exported from the device, and 2) distribute minimum FIPS 140-2 Level 2 standard cryptographic devices to Subscribers;
(l) If applicable, develop code and integrate into GlobalSign's API; and
(m) If applicable, meet all AEG system and network requirements as described in the AEG user guide.
(n) Company shall only request Certificates for which Company controls the email account associated with the address or have obtained authorization from the account holder as specified in the Mozilla CA Certificate Inclusion Policy at https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/
(o) If Company is associated with the Certificate issuance or lifecycle management of WEQ-012 v3.0 Certificates, Company shall also comply with all Registration Authority obligations stated in the GlobalSign CPS specific to NAESB WEQ-012 Certificates and the obligations stated in the NAESB WEQ-012 standard.

Company's failure to comply with any of the obligations under this Section 5 shall be a material breach of this Agreement.

6. Fees and Payments

Company shall pay to GlobalSign the applicable fees for the Service in accordance with the payment terms agreed by Company when placing its order.

Irrespective of Certificate validity period, all Certificates must be issued within 12 months of certificate pack activation.

7. LIMITED WARRANTY

GLOBALSIGN MAKES NO WARRANTY AS TO THE USE, INABILITY TO USE, DELIVERY, LICENSE, PERFORMANCE OR NONPERFORMANCE OF THE SERVICE, CERTIFICATES, DIGITAL SIGNATURES, THE SOFTWARE, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS AGREEMENT, EXPRESS OR IMPLIED. GLOBALSIGN EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT EXCEPT FOR DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THE CPS) ON THE VERIFIED INFORMATION AS OF THE ISSUANCE OF THE CERTIFICATE UP TO AN AMOUNT SET FORTH UNDER THE WARRANTY POLICY (AVAILABLE AT http://www.globalsign.com/repository/) FOR PERSONALSIGN 2 PRO, AATL, MOBILE AND ADOBE CDS CERTIFICATE. NOTWITHSTANDING THE FOREGOING, GLOBALSIGN WILL NOT BE LIABLE IN ANY CASE IF 1) THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILFULL MISCONDUCT OF THE SUBSCRIBER, OR 2) THERE IS A BREACH OF THIS AGREEMENT BY THE SUBSCRIBER.

8. LIMITATION OF LIABILITY

Each party's aggregate liability to the other party for any claim arising out of or relating to this Agreement or the use of or inability to use the Service will in no event exceed the amount of fees paid by Company for the Service within the one (1) year period immediately prior to the event that gave rise to its claim.

9. LIMITATION OF DAMAGES

Except for fraud or willful misconduct, in no event shall GlobalSign be liable for any indirect, incidental or consequential damages, or for any loss of profits, loss of data, or other indirect,

consequential or punitive damages arising from or in connection with the use, delivery, license, performance or nonperformance of the Service, Certificates, Digital Signatures, or any other transactions or services offered or contemplated by this Agreement, even if GlobalSign has been advised of the possibility of such damages.

10. Term and Termination

10.1 Term
This Agreement shall commence as of the Effective Date and continue for a period of one (1) year (the "Initial Term"). This Agreement will renew automatically on the same terms and conditions for additional successive periods of one (1) year (each a "Renewal Term") unless either party provides the other written notice of its intention not to renew at least sixty (60) days prior to the end of the then-applicable term.

10.2 Termination
This Agreement may be terminated by GlobalSign due to the Company's failure to perform any of its obligations under this Agreement if such breach is not cured within thirty (30) days after receipt of notice thereof from GlobalSign.

11. Effect of Termination

Upon the expiration or termination of this Agreement for any reason, the Company shall have no right to issue any additional Certificates. Notwithstanding the foregoing, any use or effectiveness of the Certificates issued prior to the termination of this Agreement shall not be affected thereby, and terms and conditions of this Agreement shall continue to apply to Certificates issued prior to the termination until the expiration or earlier revocation of such Certificates.

12. Miscellaneous

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

12.2 Assignment
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 a Certificate shall be transferable or assignable by Company or Subscriber. Any such purported transfer or assignment shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

12.3 Severability
If and to the extent that any court holds any provision of this Agreement to be unenforceable, such unenforceable provision shall be stricken and the remainder of this Agreement shall not be affected thereby. The parties shall in good faith attempt to replace any unenforceable provision of this Agreement with a provision that is enforceable and that comes as close as possible to expressing the intention of the original provision.

12.4 Entire Agreement
This Agreement and the CPS, which is incorporated by reference hereto and is available at www.globalsign.com/repository, constitute the entire understanding and agreement of the parties hereto with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements or understandings between the parties.

12.5 Trade Names, Logos

By reason of this Agreement or the performance hereof, Company and GlobalSign shall not acquire any 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 such rights to such trademarks, trade names, logos or product designation.