



GlobalSign Service Agreement for ePKI (UK)

Version 1.1

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE ePKI SERVICE. BY USING THE ePKI SERVICE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY CANCEL THE ORDER WITHIN 7 DAYS TO GLOBALSIGN FOR A FULL REFUND. 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 ("GlobalSign") and the organization agreeing to this Agreement ("Local RA" or "LRA") upon LRA agreeing to terms and conditions stated herein through clicking the agree button below (the "Effective Date"). Except for governing law and jurisdiction under the GlobalSign Certification Practice Statement (CPS), GlobalSign CPS is incorporated by reference hereto and is available at www.globalsign.com/repository.

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.

Digital Certificate

A record that, at a minimum (a) identifies the Certification Authority issuing it, (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber, (d) identifies its operational period, and (e) contains a serial number and is Digitally Signed by the issuing Certification Authority.

Certification Authority ("CA")

GlobalSign or an entity which is certified by GlobalSign to issue Digital Certificate.

Digital Signature

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

Local Registration Authority OR LRA

An entity appointed (other than GlobalSign) that has the responsibility to identify and authenticate Subscribers requesting Digital Certificates. The LRA does not issue Digital Certificates. It merely requests the issuance of Digital Certificates on behalf of

Subscriber whose identity it has verified. Under this Agreement, the organization agreeing to this Agreement shall be the LRA.

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.

Subscriber

An individual or an organization who (a) is the subject named or identified in a Digital Certificate issued to such an individual or organization, (b) holds a Private Key that corresponds to a Public Key listed in that Digital Certificate, and (c) the individual or organization to whom Digitally Signed messages verified by reference to such Digital Certificate are to be attributed.

Service

The ePKI service provided by GlobalSign to LRA and Subscribers. Description of the Service is set forth under Section 3 below.

Trustworthy System

Trustworthy System means computer hardware, software, and procedures that (a) are reasonably secure from intrusion and misuse, (b) provide a reasonable level of availability, reliability, and correct operation, (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

2. Authority to Use ePKI service

Grant of Authority

As of the Effective Date, GlobalSign hereby grants to LRA the authority to use ePKI service under the terms set forth in this Agreement.

Limitations on Authority

LRA shall use the ePKI service only for purposes that are permitted by (a) this agreement and GlobalSign CPA, and (b) any applicable laws and regulations, including any laws regarding the export of data or software.

3. Services Provided by GlobalSign

GlobalSign shall be the CA) issuing the Digital Certificate upon approval of LRA who shall authenticate and validate the application and enrollment information of Subscriber. LRA shall (1) receive and process the Digital Certificate application from Subscriber, (2) send an acknowledgment to Subscriber of either the approval or rejection of the Digital Certificate application, (3) if the Digital Certificate application is approved, instruct GlobalSign to issue the Digital Certificate, and (d) process all requests for revocation of the Digital Certificate upon the receipt of an authenticated request from Subscriber. Subscriber or LRA shall have the right to revoke the Digital Certificate upon, (1) any change to the information on the Digital Certificate or the Digital Certificate application,

including, but not limited to the change of the name or domain name registration of Subscriber or (2) any actual or suspected loss, disclosure, or other compromise of Subscriber's Private Key.

This Service is provided as a web-based service. If this Service is used in conjunction with any third party products, GlobalSign may specify certain specifications to be met by LRA.

a. ePKI for DocumentSign Digital IDs for Adobe PDF

Specific features include:

- Certificate management portal capable of issuing Adobe CDS Digital IDs to Subscriber for use in conjunction with Adobe PDF and third party cryptographic products in compliance with the GlobalSign CPS for Adobe Certified Document Services (CDS)
- Reports depicting Digital Certificate enrollment and issuance status
- Revocation capability
- Email management and template customization
- Optional bulk shipment of minimum FIPS 140-1 Level 2 standards cryptographic devices
- Optional time-stamping support

b. ePKI for PersonalSign Digital IDs

Specific features include:

- Certificate management portal capable of issuing Digital Certificate to Subscriber for use in conjunction products that utilize Digital Certificate for authentication and digital signing among other applications in compliance with the GlobalSign CPS.
- Reports depicting Digital Certificate enrollment and issuance status
- Revocation capability
- Email management and template customization
- Optional Bulk shipment of minimum FIPS 140-1 Level 2 standards cryptographic devices

4. LRA's Obligations

LRA shall comply with each of the following obligations:

- (1) Perform the registration authority functions necessary for issuance of the Digital Certificate provided by the Service, including application process of the Digital Certificate, and be solely responsible for verifying the identity and information stipulated in the Digital Certificate;
- (2) Appoint administrator(s) with an authority to review and approve requests for Digital Certificate and to order, manage, and revoke the Digital Certificate provided under the Service;
- (3) Ensure the digital ID or user name and password issued to the administrator which enables an individual to perform the local registration authority functions (collectively, the "Administrator Digital ID") is secure and accessible only by the individual(s) authorized to use;

- (4) Ensure that information provided on the enrollment requests is complete and accurate;
- (5) Protect the confidentiality of the private keys from unauthorized use, access or disclosure by use of the Trustworthy System, and require the same of Subscriber;
- (6) Promptly revoke or request GlobalSign to revoke the Digital Certificate in the event of 1) Subscriber's violation of this Agreement, or 2) any actual or suspected loss, disclosure, or other compromise of the private key;
- (7) Promptly request that GlobalSign revoke the Administrator Digital ID upon 1) any change to the information on the Administrator Digital ID, or 2) any actual or suspected loss, disclosure, or other compromise of the Administrator Digital ID;
- (8) Ensure that LRA and Subscriber enter into an agreement that governs the Subscriber's use of the Digital ID ("Subscriber Agreement"), and that all Subscribers accept and comply with the terms and conditions of the Subscriber Agreement;
- (9) Act as the sole intermediary for all communications with Subscriber;
- (10) In the case of ePKI for DocumentSign Digital IDs for Adobe CDS, 1) ensure and enforce all private key generations are performed on the required cryptographic device (as defined in the GlobalSign CPS for Adobe Certified Document Services (CDS)) and are never exported from the device, and 2) distribute minimum FIPS 140-1 Level 2 standards cryptographic devices to Subscriber;
- (11) If applicable, develop code and integrate into GlobalSign's API; and
- (12) Create and keep records of 1) Subscriber identity verification and 2) certificate revocation;
- (13) Cooperate to audit by either GlobalSign or a third party auditor designated by GlobalSign.

GlobalSign may provide LRA with certain software components solely for LRA's use in connection with the Service during the term of this Agreement. In such case, LRA shall not, and LRA shall ensure that Subscriber will not: (1) alter, copy, or duplicate any aspect of the software; or (2) modify, adapt, translate, decompile, disassemble or reverse engineer the software or any part thereof in any form whatsoever, or otherwise attempt to derive source code or create derivative works there from, and shall not authorize or allow any third party to do any of the above.

Failure to comply with any of the obligations under this Section 4 shall be a breach of this Agreement.

5. Fees

LRA shall pay to GlobalSign the applicable fees associated with the Service in accordance with the payment terms agreed between the parties.

6. DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY

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, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE OR NONPERFORMANCE OF DIGITAL CERTIFICATES, DIGITAL SIGNATURES, OR ANY

OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS AGREEMENT, EXCEPT FOR DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THE CPS) ON THE VERIFIED INFORMATION AS OF THE ISSUANCE OF THE DIGITAL CERTIFICATE UP TO AN AMOUNT SET FORTH UNDER WARRANTY POLICY (AVAILABLE UNDER <http://www.globalsign.com/repository/>) FOR PERSONALSIGN 2 PRO AND ADOBE CDS CERTIFICATE. NOTWITHSTANDING, GLOBALSIGN WILL NOT BE LIABLE IN ANY CASE IF 1) THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILFULL MIDCONDUCT OF THE SUBSCRIBER, OR 2) THERE IS A BREACH OF THIS AGREEMENT BY THE SUBSCRIBER.

7. Term and Termination

7.1 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 a written notice of its intention not to renew at least sixty (60) days prior to the end of the then-applicable term.

7.2 This Agreement shall terminate on the earliest of:

- (1) One year from the Effective Date; or
- (2) Failure by LRA 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.

8. Effect of Termination

Upon the termination of this Agreement for any reason, LRA shall have no right in issuing any new Digital Certificate. Notwithstanding the foregoing, any use or effectiveness of the Digital Certificate prior to the termination of this Agreement shall not be affected thereby, and terms and conditions of this Agreement shall continuously apply to the Digital Certificate issued prior to the termination until maturity of such Digital Certificate.

9. Miscellaneous Provisions

Governing Laws and Jurisdiction

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 Subscriber's Digital Certificate shall be assignable by LRA or Subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application

of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto.

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.

Entire Agreement

This Agreement constitutes 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.

Trade Names, Logos.

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

10. NOTICE

LRA shall notify GlobalSign through any of our international offices as listed on <http://www.globalsign.com/company/contact.htm> immediately in case of any error in the Digital Certificate. Without notification from LRA or Subscriber within 7 days from receipt of the Digital Certificate, the Digital Certificate shall be deemed accepted.