



Trust is what we do.

SSL.com Enterprise PKI Service Agreement

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 epki@ssl.com

This SSL.com Enterprise PKI Service Agreement ("Agreement") shall become effective between SSL.com and the organization agreeing to this Agreement ("Company") upon your acceptance of the terms and conditions stated herein (the "Effective Date"). Acceptance may be confirmed by agreement via SSL.com systems during the ordering process OR by any other means deemed mutually acceptable, including a request and confirmation of acceptance via email sent between SSL.com and a valid email address for the Company.

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.

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".

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of SSL.com or is SSL.com.

Authorized Certification Authority (ACA): a Certification Authority accredited to operate under the technical, managerial and policy controls found in the applicable requirements¹ and in the root store program policies of certificate consumers². Additionally, the ACA is found to be compliant with these standards based on annual WebTrust audits administered by third-party auditing services recognized by these certificate consumers.

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. Unless otherwise stated, SSL.com is the CA for purposes of this document.

3100 Richmond Ave. Suite 405
Houston, TX 77098
Phone: +1-775-237-8434
Fax: 832 201 7706
Email: epki@ssl.com

¹For all certificate types except document signing, this entails requirements published and maintained by CA/Browser Forum (www.cabforum.org), such as the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates or the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.

CP/CPS: SSL.com's Certificate Policy and Certification Practice Statement, available at <http://www.SSL.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: Role assigned to a natural person by the LRA for identifying and authenticating Subscribers and to perform administrator tasks associated with the life cycle management of Certificates issued from the Service, including requests for renewal, revocation, re-issuance, and any required reporting and documentation functions.

SSL.com: The entity to which Company applied for the Service. SSL.com is the CA providing Certificates issued through the Service.

Key Pair: The Private Key and its associated Public Key.

Local Registration Authority (LRA): The function through which Subscribers requesting Certificates are identified and authenticated by an EPKI Administrator appointed by the Company. The LRA does not issue Certificates but requests the issuance of Certificates on behalf of Subscriber whose identity the LRA has verified via the EPKI Administrator. Under this Agreement, Company shall be the LRA for the Service provided to that Company for all Subscribers operating under that Company, including those for which Company serves as Applicant Representative.

North American Energy Standards Board (NAESB): the industry forum for the development and promotion of standards which will lead to a seamless marketplace for wholesale and retail natural gas and electricity, as recognized by its customers, business community, participants, and regulatory entities.

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.

Service: The EPKI service provided by SSL.com to Company and Subscribers, through which Company (as LRA) applies for, manages, and uses Certificates, and SSL.com (as CA) generates and issues such Certificates and provides related CA services to Company on an out-source basis.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.

3100 Richmond Ave. Suite 405
Houston, TX 77098
Phone: +1-775-237-8434
Fax: 832 201 7706
Email: epki@ssl.com

²This includes web browser software vendors such as Apple, Google, Microsoft, Mozilla, as well as document signing software vendors such as Adobe and code signing software vendors such as Microsoft and Oracle.

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

SSL.com 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 SSL.com

SSL.com shall issue Certificates upon approval of the EPKI Administrator who shall authenticate and validate the application and enrollment information of the Subscribers.

4. COMPANY'S OBLIGATIONS

Company shall:

1. Appoint an EPKI Administrator to set up and maintain the Service, including any required registration, ordering, and configuration required to utilize the Service, and performing the local 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;
2. At Company's option, appoint an EPKI Administrator with authority to review and optionally approve requests for Certificates and to order, manage, and request revocation of the Certificates provided under the Service. The EPKI Administrator may complete the enrollment process for the Applicant provided that a) the email address associated with the Applicant is owned and/or controlled by Company or b) the EPKI Administrator has explicit authorization from the Applicant to serve as Applicant Representative;
3. Ensure the access credentials (typically, username and password) issued to the EPKI Administrator which enables an individual to perform the Local Registration Authority functions is secure and accessible only by the authorized individual(s);

4. Ensure that information provided on the enrollment requests is complete and accurate;
5. Protect the confidentiality of Private Keys from unauthorized use, access or disclosure by use of the Trustworthy System, and require the same of Subscriber;
6. Promptly request revocation of any affected 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;
7. Promptly change access credentials upon 1) any change in status or designation of Company's EPKI Administrator, or 2) any actual or suspected loss, disclosure, or other compromise of these credentials;
8. Enter into and ensure compliance by each Subscriber with the terms of the Subscriber Agreement, either directly through the Service or through Company's own workflow process, as found at <https://www.SSL.com/repository/>
9. Create and keep all records relevant to Company's functions as an LRA, including but not limited to records of: a) Subscriber identity verification b) Certificate revocation requests sent to SSL.com and c) authorizations to serve as Applicant Representative;
10. Request only Certificates for which Company a) controls the email account associated with the address or b) has obtained documented authorization from the account holder for Company to serve as Applicant Representative;
11. Comply with all Registration Authority obligations stated in the SSL.com CPS which are specific to NAESB WEQ-012 Certificates and the obligations stated in the NAESB WEQ-012 standard.

Failure of the Company to comply with any of the obligations in the above Section shall be considered a material breach of this Agreement.

5. FEES AND PAYMENTS

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

6. LIMITED WARRANTY

SSL.COM 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. SSL.COM 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 SSL.COM CP/CPS) ON THE VERIFIED INFORMATION AS OF THE ISSUANCE OF THE CERTIFICATE UP TO AN AMOUNT SET FORTH UNDER THE WARRANTY POLICY (AVAILABLE AT <https://www.ssl.com/purchasing-policy-and-warranty-coverage/>)

7. 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.

8. LIMITATION OF DAMAGES

Except for fraud or willful misconduct, in no event shall SSL.com 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 SSL.com has been advised of the possibility of such damages.

9. TERM AND TERMINATION

9.1 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.

9.2 Termination

This Agreement may be terminated by SSL.com 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 SSL.com.

10. Effect of Termination

Upon the expiration or termination of this Agreement for any reason, the Company shall have no right to request 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.

11. MISCELLANEOUS

11.1 Governing Law and Jurisdiction

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

11.2 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 SSL.com to terminate this Agreement.

11.3 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.

11.4 Entire Agreement

This Agreement and the SSL.com CP/CPS, which is incorporated by reference hereto and is available at www.SSL.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.

11.5 Trade Names, Logos

By reason of this Agreement or the performance hereof, Company and SSL.com 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.